

14.10.99

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

REC'D 29 OCT 1999

WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

1998年11月4日

出願番号

Application Number:

平成10年特許願第313020号

出願人

Applicant (s):

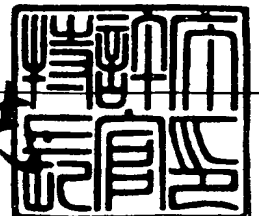
ソニー株式会社

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a)OR(b)

1999年8月24日

特許庁長官
Commissioner,
Patent Office

山佐平



出証番号 出証特平11-3059151

【書類名】	特許願
【整理番号】	9800814907
【提出日】	平成10年11月 4日
【あて先】	特許庁長官殿
【国際特許分類】	H04K 1/00
【発明の名称】	情報処理装置および方法、提供媒体、並びに情報記憶媒体
【請求項の数】	13
【発明者】	
【住所又は居所】	東京都品川区北品川 6丁目 7番 35号 ソニー株式会社 内
【氏名】	石橋 義人
【発明者】	
【住所又は居所】	東京都品川区北品川 6丁目 7番 35号 ソニー株式会社 内
【氏名】	浅野 智之
【特許出願人】	
【識別番号】	000002185
【氏名又は名称】	ソニー株式会社
【代表者】	出井 伸之
【代理人】	
【識別番号】	100082131
【弁理士】	
【氏名又は名称】	稲本 義雄
【電話番号】	03-3369-6479
【手数料の表示】	
【予納台帳番号】	032089
【納付金額】	21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708842

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置および方法、提供媒体、並びに情報記憶媒体

【特許請求の範囲】

【請求項 1】 暗号化されている情報を復号して利用する情報処理装置において、

前記情報の使用の許諾条件を示す情報を生成する許諾条件情報生成手段と、
前記許諾条件を示す情報の認証情報を生成する認証情報生成手段と、
前記認証情報を記憶する記憶手段と
を備えることを特徴とする情報処理装置。

【請求項 2】 前記記憶手段は、耐タンパー性を有する構造であることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 暗号化されている情報を復号して利用する情報処理方法において、

前記情報の使用の許諾条件を示す情報を生成する許諾条件情報生成ステップと、
前記許諾条件を示す情報の認証情報を生成する認証情報生成ステップと、
前記認証情報を記憶する記憶ステップと
を含むことを特徴とする情報処理方法。

【請求項 4】 暗号化されている情報を復号して利用する情報処理装置に、
前記情報の使用の許諾条件を示す情報を生成する許諾条件情報生成ステップと、
前記許諾条件を示す情報の認証情報を生成する認証情報生成ステップと、
前記認証情報を記憶する記憶ステップと
を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項 5】 装着された情報記憶媒体に情報を記憶させて利用する情報処理装置において、

前記情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成手段と、

前記認証情報を記憶する記憶手段と、

前記関連情報から、他の認証情報を生成し、前記記憶手段が記憶している前記認証情報との一致を検証する検証手段と、

前記情報記憶媒体と相互認証する相互認証手段と
を備えることを特徴とする情報処理装置。

【請求項 6】 前記情報を暗号化する暗号化手段
を更に備えることを特徴とする請求項 5 に記載の情報処理装置。

【請求項 7】 前記認証情報を暗号化する暗号化手段
を更に備えることを特徴とする請求項 5 に記載の情報処理装置。

【請求項 8】 前記記憶手段が記憶する暗号化されている前記認証情報を復号する復号手段

を更に備えることを特徴とする請求項 7 に記載の情報処理装置。

【請求項 9】 装着された情報記憶媒体に情報を記憶させて利用する情報処理装置の情報処理方法において、

前記情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成ステップと、

前記認証情報を記憶する記憶ステップと、

前記関連情報から、他の認証情報を生成し、前記記憶ステップで記憶した前記認証情報との一致を検証する検証ステップと、

前記情報記憶媒体と相互認証する相互認証ステップと
を含むことを特徴とする情報処理方法。

【請求項 10】 装着された情報記憶媒体に情報を記憶させて利用する情報処理装置に、

前記情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成ステップと、

前記認証情報を記憶する記憶ステップと、

前記関連情報から、他の認証情報を生成し、前記記憶ステップで記憶した前記認証情報との一致を検証する検証ステップと、

前記情報記憶媒体と相互認証する相互認証ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項 11】 暗号化された情報を記憶し、情報処理装置に装着される情報記憶媒体において、

前記情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成手段と、

前記認証情報を記憶する記憶手段と、

前記関連情報から、他の認証情報を生成し、前記記憶手段が記憶している前記認証情報との一致を検証する検証手段と、

前記情報処理装置と相互認証する相互認証手段と

を備えることを特徴とする情報記憶媒体。

【請求項 12】 前記認証情報を暗号化する暗号化手段

を更に備えることを特徴とする請求項 11 に記載の情報記憶媒体。

【請求項 13】 前記記憶手段が記憶する暗号化されている前記認証情報を復号する復号手段

を更に備えることを特徴とする請求項 11 に記載の情報記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置および方法、提供媒体、並びに情報記憶媒体に関し、特に、暗号化された情報を復号する情報処理装置および方法、提供媒体、並びに情報記憶媒体に関する。

【0002】

【従来の技術】

音楽などの情報を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザは、その情報処理装置で情報を復号して、再生するシステムがある。ユーザは、例えば再生のみの利用、または5回の再生など、情報毎に利用内容を定め、情報を利用することができる。

【0003】

【発明が解決しようとする課題】

しかし、利用内容を示す情報を書き換えることにより、所定の料金を支払わずに、例えば、再生の回数の制限を解除する、または、再生のみからコピーも可能とするなど、利用内容を変更することができる。

【0004】

本発明はこのような状況に鑑みてなされたものであり、利用内容を示す情報の書き換えを検知し、対応できるようにすることを目的とする。

【0005】

【課題を解決するための手段】

請求項1に記載の情報処理装置は、情報の使用の許諾条件を示す情報を生成する許諾条件情報生成手段と、許諾条件を示す情報の認証情報を生成する認証情報生成手段と、認証情報を記憶する記憶手段とを備えることを特徴とする。

【0006】

請求項3に記載の情報処理方法は、情報の使用の許諾条件を示す情報を生成する許諾条件情報生成ステップと、許諾条件を示す情報の認証情報を生成する認証情報生成ステップと、認証情報を記憶する記憶ステップとを含むことを特徴とする。

【0007】

請求項4に記載の提供媒体は、情報処理装置に、情報の使用の許諾条件を示す情報を生成する許諾条件情報生成ステップと、許諾条件を示す情報の認証情報を生成する認証情報生成ステップと、認証情報を記憶する記憶ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0008】

請求項5に記載の情報処理装置は、情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成手段と、認証情報を記憶する記憶手段と、関連情報から、他の認証情報を生成し、記憶手段が記憶している認証情報との一致を検証する検証手段と、情報記憶媒体と相互認証する相互認証手段とを備えることを特

徴とする。

【0009】

請求項9に記載の情報処理方法は、情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成ステップと、認証情報を記憶する記憶ステップと、関連情報から、他の認証情報を生成し、記憶ステップで記憶した認証情報との一致を検証する検証ステップと、情報記憶媒体と相互認証する相互認証ステップとを含むことを特徴とする。

【0010】

請求項10に記載の提供媒体は、情報処理装置に、情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成ステップと、認証情報を記憶する記憶ステップと、関連情報から、他の認証情報を生成し、記憶ステップで記憶した認証情報との一致を検証する検証ステップと、情報記憶媒体と相互認証する相互認証ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0011】

請求項11に記載の情報記憶媒体は、情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成手段と、認証情報を記憶する記憶手段と、関連情報から、他の認証情報を生成し、記憶手段が記憶している認証情報との一致を検証する検証手段と、情報処理装置と相互認証する相互認証手段とを備えることを特徴とする情報記憶媒体。

【0012】

請求項1に記載の情報処理装置、請求項3に記載の情報処理方法、および請求項4に記載の提供媒体においては、情報の使用の許諾条件を示す情報を生成し、許諾条件を示す情報の認証情報を生成し、認証情報を記憶する。

【0013】

~~請求項5に記載の情報処理装置、請求項9に記載の情報処理方法、および請求項10に記載の提供媒体においては、情報の利用のときに必要な関連情報の認証情報を生成し、認証情報を記憶し、関連情報から、他の認証情報を生成し、記憶している認証情報との一致を検証し、情報記憶媒体と相互認証する。~~

【0014】

請求項 11 に記載の情報記憶媒体においては、認証情報生成手段が、情報の利用のときに必要な関連情報の認証情報を生成し、記憶手段が認証情報を記憶し、検証手段が、関連情報から、他の認証情報を生成し、記憶手段が記憶している認証情報との一致を検証し、相互認証手段が、情報処理装置と相互認証する。

【0015】

【発明の実施の形態】

以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【0016】

すなわち、請求項 1 に記載の情報処理装置は、情報の使用の許諾条件を示す情報を生成する許諾条件情報生成手段（例えば、図 10 の課金処理モジュール 72）と、許諾条件を示す情報の認証情報を生成する認証情報生成手段（例えば、図 10 の復号／暗号化モジュール 74）と、認証情報を記憶する記憶手段（例えば、図 10 の記憶モジュール 73）とを備えることを特徴とする。

【0017】

請求項 5 に記載の情報処理装置は、情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成手段（例えば、図 30 の復号／暗号化モジュール 74）と、認証情報を記憶する記憶手段（例えば、図 30 の記憶モジュール 73）と、関連情報から、他の認証情報を生成し、記憶手段が記憶している認証情報との一致を検証する検証手段（例えば、図 30 のデータ検査モジュール 114）と、情報記憶媒体と相互認証する相互認証手段（例えば、図 30 の相互認証モジュール 71）とを備えることを特徴とする。

【0018】

請求項 11 に記載の情報記憶媒体は、情報の利用のときに必要な関連情報の認証情報を生成する認証情報生成手段（例えば、図 30 のデータ検査部 138）と

、認証情報を記憶する記憶手段（例えば、図30の記憶部135）と、関連情報から、他の認証情報を生成し、記憶手段が記憶している認証情報との一致を検証する検証手段（例えば、図30のデータ検査部138）と、情報処理装置と相互認証する相互認証手段（例えば、図30の相互認証部133）とを備えることを特徴とする情報記憶媒体。

【0019】

図1は、本発明を適用したEMD(Electronic Music Distribution:電子音楽配信)システムを説明する図である。このシステムでユーザに配信されるコンテンツ(Content)とは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。EMDサービスセンタ1は、コンテンツプロバイダ2、ユーザホームネットワーク5等に配送用鍵Kdを送信し、ユーザホームネットワーク5から、コンテンツの利用に応じた課金情報等を受信し、利用料金を精算し、コンテンツプロバイダ2およびサービスプロバイダ3への利益分配の処理を行う。

【0020】

コンテンツプロバイダ2は、デジタル化されたコンテンツを有し、自己のコンテンツであることを証明するためのウォーターマーク（電子透かし）をコンテンツに挿入し、コンテンツを圧縮し、および暗号化し、所定の情報を付加して、サービスプロバイダ3に送信する。

【0021】

サービスプロバイダ3は、専用のケーブルネットワーク、インターネット、または衛星などから構成されるネットワーク4を介して、コンテンツプロバイダ2から供給されたコンテンツに価格を付して、ユーザホームネットワーク5に送信する。

【0022】

ユーザホームネットワーク5は、サービスプロバイダ3から価格を付して送付されたコンテンツを入手し、コンテンツを復号、再生して利用するとともに課金処理を実行する。課金処理により得られた課金情報は、ユーザホームネットワーク5が配送用鍵KdをEMDサービスセンタ1から入手する際、EMDサービスセンタ

1 に送信される。

【0023】

図2は、EMDサービスセンタ1の機能の構成を示すブロック図である。サービスプロバイダ管理部11は、サービスプロバイダ3に利益分配の情報を供給するとともに、コンテンツプロバイダ2から供給されるコンテンツに付される情報（取扱方針）が暗号化されている場合、サービスプロバイダ3に配送用鍵Kdを送信する。コンテンツプロバイダ管理部12は、コンテンツプロバイダ2に配送用鍵Kdを送信するとともに、利益分配の情報を供給する。著作権管理部13は、ユーザホームネットワーク5のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC(Japanese Society for Rights of Authors, Composers and Publishers:日本音楽著作権協会)に送信する。鍵サーバ14は、配送用鍵Kdを記憶しており、コンテンツプロバイダ管理部12、またはユーザ管理部18等を介して、配送用鍵Kdをコンテンツプロバイダ2、またはユーザホームネットワーク5等に供給する。ユーザ管理部18は、ユーザホームネットワーク5のコンテンツの利用の実績を示す情報である課金情報、そのコンテンツに対応する価格情報、およびそのコンテンツに対応する取扱方針を入力し、経歴データ管理部15に記憶させる。

【0024】

EMDサービスセンタ1からコンテンツプロバイダ2およびユーザホームネットワーク5を構成するレシーバ51（図10で後述する）への、配送用鍵Kdの定期的な送信の例について、図3乃至図6を参照に説明する。図3は、コンテンツプロバイダ2がコンテンツの提供を開始し、ユーザホームネットワーク5を構成するレシーバ51がコンテンツの利用を開始する、1998年1月における、EMDサービスセンタ1が有する配送用鍵Kd、コンテンツプロバイダ2が有する配送用鍵Kd、およびレシーバ51が有する配送用鍵Kdを示す図である。

【0025】

図3の例において、配送用鍵Kdは、暦の月の初日から月の末日まで、使用可能であり、たとえば、所定のビット数の乱数である” a a a a a a a a ”の値を有するバージョン1である配送用鍵Kdは、1998年1月1日から1998年

1月31日まで使用可能（すなわち、1998年1月1日から1998年1月31日の期間にサービスプロバイダ3がユーザホームネットワーク5に配布するコンテンツを暗号化するコンテンツ鍵Kcoは、バージョン1である配送用鍵Kdで暗号化されている）であり、所定のビット数の乱数である”bbbbbbbb”の値を有するバージョン2である配送用鍵Kdは、1998年2月1日から1998年2月28日まで使用可能（すなわち、その期間にサービスプロバイダ3がユーザホームネットワーク5に配布するコンテンツを暗号化するコンテンツ鍵Kcoは、バージョン1である配送用鍵Kdで暗号化されている）である。同様に、バージョン3である配送用鍵Kdは、1998年3月中に使用可能であり、バージョン4である配送用鍵Kdは、1998年4月中に使用可能であり、バージョン5である配送用鍵Kdは、1998年5月中に使用可能であり、バージョン6である配送用鍵Kdは、1998年6月中に使用可能である。

【0026】

コンテンツプロバイダ2がコンテンツの提供を開始するに先立ち、EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年1月から1998年6月まで利用可能な、バージョン1乃至バージョン6の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、記憶する。6月分の配送用鍵Kdを記憶するのは、コンテンツプロバイダ2は、コンテンツを提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

【0027】

また、レシーバ51がコンテンツの利用を開始するに先立ち、EMDサービスセンタ1は、レシーバ51に、1998年1月から1998年3月まで、利用可能なバージョン1乃至バージョン3である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、記憶する。3月分の配送用鍵Kdを記憶するのは、レシーバ51が、EMDサービスセンタ1に接続できないなどのトラブルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できない等の事態を避けるためであり、また、EMDサービスセンタ1への接続の頻度を低くし、ユーザホームネットワーク5の負荷を低減するためである。

【0028】

1998年1月1日から1998年1月31日の期間には、バージョン1である配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0029】

1998年2月1日における、EMDサービスセンタ1の配送用鍵K dのコンテンツプロバイダ2、およびレシーバ51への送信を図4で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年2月から1998年7月まで利用可能な、バージョン2乃至バージョン7の6つの配送用鍵K dを送信し、コンテンツプロバイダ2は、6つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年2月から1998年4月まで、利用可能なバージョン2乃至バージョン4である3つの配送用鍵K dを送信し、レシーバ51は、3つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵K dをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵K dを利用できるようにするためである。

【0030】

1998年2月1日から1998年2月28日の期間には、バージョン2である配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0031】

1998年3月1日における、EMDサービスセンタ1の配送用鍵K dのコンテンツプロバイダ2、およびレシーバ51への送信を図5で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年3月から1998年8月まで利用可能な、バージョン3乃至バージョン8の6つの配送用鍵K dを送信し、コンテンツプロバイダ2は、6つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセ

ンタ 1 は、レシーバ 5 1 に、1998 年 3 月から 1998 年 5 月まで、利用可能なバージョン 3 乃至バージョン 5 である 3 つの配送用鍵 K d を送信し、レシーバ 5 1 は、3 つの配送用鍵 K d を受信し、受信前に記憶していた配送用鍵 K d に上書きし、新たな配送用鍵 K d を記憶する。EMD サービスセンタ 1 は、バージョン 1 である配送用鍵 K d およびバージョン 2 である配送用鍵 K d をそのまま記憶する。

【0032】

1998 年 3 月 1 日から 1998 年 3 月 31 日の期間には、バージョン 3 である配送用鍵 K d が、EMD サービスセンタ 1、コンテンツプロバイダ 2、ユーザホームネットワーク 5 を構成するレシーバ 5 1 で利用される。

【0033】

1998 年 4 月 1 日における、EMD サービスセンタ 1 の配送用鍵 K d のコンテンツプロバイダ 2、およびレシーバ 5 1 への送信を図 6 で説明する。EMD サービスセンタ 1 は、コンテンツプロバイダ 2 に、1998 年 4 月から 1998 年 9 月まで利用可能な、バージョン 4 乃至バージョン 9 の 6 つの配送用鍵 K d を送信し、コンテンツプロバイダ 2 は、6 つの配送用鍵 K d を受信し、受信前に記憶していた配送用鍵 K d に上書きし、新たな配送用鍵 K d を記憶する。EMD サービスセンタ 1 は、レシーバ 5 1 に、1998 年 4 月から 1998 年 6 月まで、利用可能なバージョン 3 乃至バージョン 5 である 3 つの配送用鍵 K d を送信し、レシーバ 5 1 は、3 つの配送用鍵 K d を受信し、受信前に記憶していた配送用鍵 K d に上書きし、新たな配送用鍵 K d を記憶する。EMD サービスセンタ 1 は、バージョン 1 である配送用鍵 K d、バージョン 2 である配送用鍵 K d、およびバージョン 3 である配送用鍵 K d をそのまま記憶する。

【0034】

1998 年 4 月 1 日から 1998 年 4 月 30 日の期間には、バージョン 4 である配送用鍵 K d が、EMD サービスセンタ 1、コンテンツプロバイダ 2、ユーザホームネットワーク 5 を構成するレシーバ 5 1 で利用される。

【0035】

利益分配部 16 は、経歴データ管理部 15 から供給された、課金情報、価格情

報、および取扱方針に基づき、EMDサービスセンタ 1、コンテンツプロバイダ 2、およびサービスプロバイダ 3 の利益を算出する。相互認証部 17 は、コンテンツプロバイダ 2、サービスプロバイダ 3、およびユーザホームネットワーク 5 の所定の機器と後述する相互認証を実行する。

【0036】

ユーザ管理部 18 は、ユーザ登録データベースを有し、ユーザホームネットワーク 5 の機器から登録の要求があったとき、ユーザ登録データベースを検索し、その記録内容に応じて、その機器を登録したり、または登録を拒絶する等の処理を実行する。ユーザホームネットワーク 5 が EMD サービスセンタ 1 と接続が可能な機能を有する複数の機器から構成されているとき、ユーザ管理部 18 は、登録が可能か否かの判定の処理の結果に対応して、決済をする機器を指定し、さらに、コンテンツの利用条件を規定した登録リストをユーザホームネットワーク 5 の所定の機器に送信する。

【0037】

図 7 に示すユーザ登録データベースの例は、ユーザホームネットワーク 5 の機器の機器固有の 64 ビットからなる ID (Identification Data) を記録し、その ID に対応して (すなわち、その ID を有する機器毎に)、決済処理が可能か否か、登録が可能か否か、EMD サービスセンタ 1 と接続が可能か否か等の情報を記録する。ユーザ登録データベースに記録された登録が可能か否かの情報は、決済機関 (例えば、銀行)、またはサービスプロバイダ 3 などから供給される料金の未払い、不正処理等の情報を基に、所定の時間間隔で更新される。登録が不可と記録された ID を有する機器の登録の要求に対して、ユーザ管理部 18 は、その登録を拒否し、登録を拒否された機器は、以後、このシステムのコンテンツを利用できない。

【0038】

ユーザ登録データベースに記録された決済処理が可能か否かの情報は、その機器が、決済可能か否かを示す。ユーザホームネットワーク 5 が、コンテンツの再生またはコピーなどの利用が可能な複数の機器で構成されているとき、その中の決済処理が可能である 1 台の機器は、EMD サービスセンタ 1 に、ユーザホームネ

ットワーク 5 の EMD サービスセンタ 1 に登録されている全ての機器の、課金情報、価格情報、および取扱方針を出力する。ユーザ登録データベースに記録された EMD サービスセンタ 1 と接続が可能か否かの情報は、その機器が、EMD サービスセンタ 1 と接続が可能であるか否かを示し、接続ができないと記録された機器は、ユーザホームネットワーク 5 の他の機器を介して、EMD サービスセンタ 1 に、課金情報等を出力する。

【0039】

また、ユーザ管理部 18 は、ユーザホームネットワーク 5 の機器から課金情報、価格情報、および取扱方針が供給され、その情報を経歴データ管理部 15 に出力し、さらに、所定の処理（タイミング）で、ユーザホームネットワーク 5 の機器に、配送用鍵 K d を供給する。

【0040】

課金請求部 19 は、経歴データ管理部 15 から供給された、課金情報、価格情報、および取扱方針に基づき、ユーザへの課金を算出し、その結果を、出納部 20 に供給する。出納部 20 は、ユーザ、コンテンツプロバイダ 2、およびサービスプロバイダ 3 への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。監査部 21 は、ユーザホームネットワーク 5 の機器から供給された課金情報、価格情報、および取扱方針の正当性（すなわち、不正をしていないか）を監査する。

【0041】

図 8 は、コンテンツプロバイダ 2 の機能の構成を示すブロック図である。コンテンツサーバ 31 は、ユーザに供給するコンテンツを記憶し、ウォーターマーク付加部 32 に供給する。ウォーターマーク付加部 32 は、コンテンツサーバ 31 から供給されたコンテンツにウォーターマークを付加し、圧縮部 33 に供給する。圧縮部 33 は、ウォーターマーク付加部 32 から供給されたコンテンツを、ATRAC2 (Adaptive Transform Acoustic Coding 2) (商標) 等の方式で圧縮し、暗号化部 34 に供給する。暗号化部 34 は、圧縮部 33 で圧縮されたコンテンツを、乱数発生部 35 から供給された乱数を鍵（以下、この乱数をコンテンツ鍵 K c o と称する）として、DES (Data Encryption Standard) などの共通鍵暗号方式で暗号化し、

その結果をセキュアコンテナ作成部 38 に出力する。

【0042】

乱数発生部 35 は、コンテンツ鍵 K_c となる所定のビット数の乱数を暗号化部 34 および暗号化部 36 に供給する。暗号化部 36 は、コンテンツ鍵 K_c を EMD サービスセンタ 1 から供給された配送用鍵 K_d を使用して、DES などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部 38 に出力する。

【0043】

DES は、56 ビットの共通鍵を用い、平文の 64 ビットを 1 ブロックとして処理する暗号方式である。DES の処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。DES のすべてのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

【0044】

まず、平文の 64 ビットは、上位 32 ビットの H_0 、および下位 32 ビットの L_0 に分割される。鍵処理部から供給された 48 ビットの拡大鍵 K_1 、および下位 32 ビットの L_0 を入力とし、下位 32 ビットの L_0 を攪拌した F 関数の出力が算出される。F 関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の 2 種類の基本変換から構成されている。次に、上位 32 ビットの H_0 と、F 関数の出力が排他的論理和され、その結果は L_1 とされる。 L_0 は、 H_1 とされる。

【0045】

上位 32 ビットの H_0 および下位 32 ビットの L_0 を基に、以上の処理を 16 回繰り返し、得られた上位 32 ビットの H_{16} および下位 32 ビットの L_{16} が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

【0046】

ポリシー記憶部 37 は、コンテンツの取扱方針（ポリシー）を記憶し、暗号化されるコンテンツに対応して、取扱方針をセキュアコンテナ作成部 38 に出力する。セキュアコンテナ作成部 38 は、暗号化されたコンテンツ、暗号化されたコ

コンテンツ鍵 K_{co} 、取扱方針、並びに暗号化されたコンテンツ、暗号化されたコンテンツ鍵 K_{co} 、および取扱方針のハッシュ値をとり作成された署名、さらにコンテンツプロバイダ2の公開鍵 K_{cp} を含む証明書から構成されるコンテンツプロバイダセキュアコンテナを作成し、サービスプロバイダ3に供給する。相互認証部39は、EMDサービスセンタ1から配送用鍵 K_d の供給を受けるのに先立ち、EMDサービスセンタ1と相互認証し、また、サービスプロバイダ3へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ3と相互認証する。

【0047】

署名は、データまたは後述する証明書に付け、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

【0048】

ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

【0049】

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD4、MD5、SHA-1などが用いられる。

【0050】

次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を

使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

【0051】

公開鍵暗号の中で代表的なRSA (Rivest-Shamir-Adleman) 暗号を、簡単に説明する。まず、2つの十分に大きな素数である p および q を求め、さらに p と q の積である n を求める。 $(p-1)$ と $(q-1)$ の最小公倍数 L を算出し、更に、3以上 L 未満で、かつ、 L と互いに素な数 e を求める（すなわち、 e と L を共通に割り切れる数は、1のみである）。

【0052】

次に、 L を法とする乗算に関する e の乗法逆元 d を求める。すなわち、 d 、 e 、および L の間には、 $ed=1 \bmod L$ が成立し、 d はユークリッドの互除法で算出できる。このとき、 n と e が公開鍵とされ、 p, q , および d が、秘密鍵とされる。

【0053】

暗号文 C は、平文 M から、式(1)の処理で算出される。

$$C=M^e \bmod n \quad (1)$$

【0054】

暗号文 C は、式(2)の処理で平文 M に、復号される。

$$M=C^d \bmod n \quad (2)$$

【0055】

証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式(3)が成立するからである。

$$M=C^d=(M^e)^d=M^{(ed)} \bmod n \quad (3)$$

【0056】

秘密鍵 p と q を知っているならば、公開鍵 e から秘密鍵 d は算出できるが、公開鍵 n の素因数分解が計算量的に困難な程度に公開鍵 n の桁数を大きくすれば、公開鍵 n を知るだけでは、公開鍵 e から秘密鍵 d は計算できず、復号できない。以上のように、RSA暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とす

ることができる。

【0057】

また、公開鍵暗号の他の例である楕円曲線暗号についても、簡単に説明する。楕円曲線 $y^2=x^3+ax+b$ 上の、ある点をBとする。楕円曲線上の点の加算を定義し、 nB は、Bをn回加算した結果を表す。同様に、減算も定義する。Bと nB からnを算出することは、困難であることが証明されている。Bと nB を公開鍵とし、nを秘密鍵とする。乱数rを用いて、暗号文C1およびC2は、平文Mから、公開鍵で式(4)および式(5)の処理で算出される。

$$C1=M+rnB \quad (4)$$

$$C2=rB \quad (5)$$

【0058】

暗号文C1およびC2は、式(6)の処理で平文Mに、復号される。

$$M=C1-nC2 \quad (6)$$

【0059】

復号できるのは、秘密鍵nを有するものだけである。以上のように、RSA暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【0060】

図9は、サービスプロバイダ3の機能の構成を示すブロック図である。コンテンツサーバ41は、コンテンツプロバイダ2から供給された、暗号化されているコンテンツを記憶し、セキュアコンテナ作成部44に供給する。値付け部42は、コンテンツに対応した取扱方針を基に、価格情報を作成し、セキュアコンテナ作成部44に供給する。ポリシー記憶部43は、コンテンツプロバイダ2から供給された、コンテンツの取扱方針を記憶し、セキュアコンテナ作成部44に供給する。相互認証部45は、コンテンツプロバイダ2からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロバイダ2と相互認証し、また、ユーザホームネットワーク5へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク5と相互認証する。また、コンテンツプロバイダ2が取扱方針を配送用鍵Kdで暗号化して供給する場合、相互

認証部 45 は、EMD サービスセンタ 1 から配送用鍵 K d の供給を受け付けるのに先立ち、EMD サービスセンタ 1 と相互認証する。

【0061】

図 10 は、ユーザホームネットワーク 5 の構成を示すブロック図である。レシーバ 51 は、ネットワーク 4 を介して、サービスプロバイダ 3 からコンテンツを含んだサービスプロバイダセキュアコンテナを受信し、コンテンツを復号および伸張し、再生する。

【0062】

通信部 61 は、ネットワーク 4 を介してサービスプロバイダ 3、または EMD サービスセンタ 1 と通信し、所定の情報を受信し、または送信する。SAM (Secure Application Module) 62 は、サービスプロバイダ 3、または EMD サービスセンタ 1 と相互認証し、コンテンツの暗号を復号し、またはコンテンツを暗号化し、さらに配送用鍵 K d 等を記憶する。伸張部 63 は、コンテンツの暗号を復号し、ATRAC2 方式で伸張し、さらに所定のウォーターマークをコンテンツに挿入する。IC (Integrated Circuit) カードインターフェース 64 は、SAM 62 からの信号を所定の形式に変更し、レシーバ 51 に装着された IC カード 55 に出力し、また、IC カード 55 からの信号を所定の形式に変更し、SAM 62 に出力する。

【0063】

サービスプロバイダ 3、または EMD サービスセンタ 1 と相互認証し、課金処理を実行し、コンテンツ鍵 K c o を復号および暗号化し、さらに使用許諾条件情報等の所定のデータを記憶する SAM 62 は、相互認証モジュール 71、課金モジュール 72、記憶モジュール 73、および復号/暗号化モジュール 74 から構成される。この SAM 62 は、シングルチップの暗号処理専用 IC で構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパー性）を有する。

【0064】

相互認証モジュール 71 は、サービスプロバイダ 3、または EMD サービスセンタ 1 との相互認証を実行し、必要に応じて、一時鍵 K t e m p （セッション鍵）

を復号／暗号化モジュール 74 に供給する。課金処理モジュール 72 は、サービスプロバイダ 3 から受信したサービスプロバイダセキュアコンテナに含まれる取扱方針および価格情報（並びに、場合によっては、取扱制御情報）から、使用許諾条件情報および課金情報を生成し、記憶モジュール 73 または HDD (Hard Disk Drive) 52 に出力する。記憶モジュール 73 は、課金処理モジュール 72 または復号／暗号化モジュール 74 から供給された課金情報、および配送用鍵 K_d 等のデータを記憶し、他の機能ブロックが所定の処理を実行するとき、配送用鍵 K_d 等のデータを供給する。

【0065】

復号／暗号化モジュール 74 は、復号ユニット 91、乱数発生ユニット 92、および暗号化ユニット 93 から構成される。復号ユニット 91 は、暗号化されたコンテンツ鍵 K_{co} を配送用鍵 K_d で復号し、暗号化ユニット 93 に出力する。乱数発生ユニット 92 は、所定の桁数の乱数を発生し、保存用鍵 K_{save} として暗号化ユニット 93 および記憶モジュール 73 に出力する。ただし、一度生成して保持している場合、生成の必要はない。暗号化ユニット 93 は、復号されたコンテンツ鍵 K_{co} を、再度、保存用鍵 K_{save} で暗号化し、HDD 52 に出力する。暗号化ユニット 93 は、コンテンツ鍵 K_{co} を伸張部 63 に送信するとき、コンテンツ鍵 K_{co} を一時鍵 K_{temp} で暗号化する。

【0066】

コンテンツを復号し、伸張し、所定のウォータマークを付加する伸張部 63 は、相互認証モジュール 75、復号モジュール 76、復号モジュール 77、伸張モジュール 78、およびウォータマーク付加モジュール 79 から構成される。相互認証モジュール 75 は、SAM 62 と相互認証し、一時鍵 K_{temp} を復号モジュール 76 に出力する。復号モジュール 76 は、SAM 62 から出力され、一時鍵 K_{temp} で暗号化されたコンテンツ鍵 K_{co} を一時鍵 K_{temp} で復号し、復号モジュール 77 に出力する。復号モジュール 77 は、HDD 52 に記録されたコンテンツをコンテンツ鍵 K_{co} で復号し、伸張モジュール 78 に出力する。伸張モジュール 78 は、復号されたコンテンツを、更に ATRAC2 等の方式で伸張し、ウォータマーク付加モジュール 79 に出力する。ウォータマーク付加モジュール 79

は、コンテンツにレシーバ51を特定する所定のウォーターマークを挿入し、レコーダ53に出力したり、図示せぬスピーカに出力し、音楽を再生する。

【0067】

HDD52は、サービスプロバイダ3から供給されたコンテンツを記録する。装着された光ディスク（図示せず）にサービスプロバイダ3から供給されたコンテンツを記録し、再生するレコーダ53は、記録再生部65、SAM66、および伸張部67から構成される。記録再生部65は、光ディスクが装着され、その光ディスクにコンテンツを記録し、再生する。SAM66は、SAM62と同じ機能を有し、その説明は省略する。伸張部67は、伸張部63と同じ機能を有し、その説明は省略する。MD(Mini Disk:商標)ドライブ54は、装着された図示せぬMDにサービスプロバイダ3から供給されたコンテンツを記録し、再生する。

【0068】

ICカード55は、レシーバ51に装着され、記憶モジュール73に記憶された配送用鍵Kdおよび機器のIDなどの所定のデータを記憶する。例えば、新たなレシーバ51を購入し、今まで使用していたレシーバ51と入れ替えて使用する場合、まず、ユーザは、ICカード55に、今まで使用していたレシーバ51の記憶モジュール73に記憶されていた配送用鍵Kdなどの所定のデータを記憶させる。次に、ユーザは、そのICカード55を新たなレシーバ51に装着し、そのレシーバ51を操作して、EMDサービスセンタ1のユーザ管理部18にその新たなレシーバ51を登録する。EMDサービスセンタ1のユーザ管理部18は、ICカード55に記憶されていたデータ（今まで使用していたレシーバ51のIDなど）を基に、ユーザ管理部18が保持しているデータベースから、ユーザの氏名、使用料の払い込みに使用するクレジットカードの番号などのデータを検索し、そのデータを基に、登録の処理を実行するので、ユーザは、面倒なデータを入力する必要がない。ICカード55は、相互認証モジュール80および記憶モジュール81で構成される。相互認証モジュール80は、SAM62と相互認証する。記憶モジュール81は、ICカードインターフェース64を介して、SAM62から供給されたデータを記憶し、記憶したデータをSAM62に出力する。

【0069】

図11は、ユーザホームネットワーク5の他の構成例を示すブロック図である。この構成のレシーバ51およびレコーダ53は、図10に示した伸張部63および伸張部67を省略した構成を有する。その代わり、レコーダ53に接続されているデコーダ56が、伸張部63または伸張部67と同じ機能を有する。その他の構成は、図10における場合と同様である。

【0070】

コンテンツを復号し、伸張し、ウォータマークを付加するデコーダ56は、相互認証モジュール101、復号モジュール102、復号モジュール103、伸張モジュール104、およびウォータマーク付加モジュール105から構成される。相互認証モジュール101は、SAM62またはSAM66と相互認証し、一時鍵Ktempを復号モジュール102に出力する。復号モジュール102は、SAM62から出力され、一時鍵Ktempで暗号化されたコンテンツ鍵Kcoを一時鍵Ktempで復号し、復号モジュール103に出力する。復号モジュール103は、HDD52に記録されたコンテンツをコンテンツ鍵Kcoで復号し、伸張モジュール104に出力する。伸張モジュール104は、復号されたコンテンツを、更にATRAC2等の方式で伸張し、ウォータマーク付加モジュール105に出力する。ウォータマーク付加モジュール105は、コンテンツにデコーダ56を特定する所定のウォータマークを挿入し、レコーダ53に出力したり、図示せぬスピーカに出力し、音楽を再生する。

【0071】

図12は、EMDサービスセンタ1、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の間で送受信される情報を説明する図である。コンテンツプロバイダ2は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Kco、取扱方針、および署名をコンテンツプロバイダセキュアコンテナ（その詳細は図13を参照して後述する）に格納し、さらにコンテンツプロバイダセキュアコンテナにコンテンツプロバイダ2の証明書（その詳細は図14を参照して後述する）を付して、サービスプロバイダ3に送信する。コンテンツプロバイダ2はまた、取扱方針、および署名にコンテンツプロバイダ2の証明

書を付して、EMDサービスセンタ 1 に送信する。

【0072】

サービスプロバイダ 3 は、受信したコンテンツプロバイダセキュアコンテナに含まれる取扱方針を基に価格情報を生成し、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 K c o、取扱方針、価格情報、および署名をサービスプロバイダセキュアコンテナ（その詳細は図 15 を参照して後述する）に格納し、さらにサービスプロバイダセキュアコンテナにサービスプロバイダ 3 の証明書（その詳細は図 16 を参照して後述する）を付して、ユーザホームネットワーク 5 に送信する。サービスプロバイダ 3 はまた、価格情報、および署名にサービスプロバイダ 3 の証明書を付して、EMDサービスセンタ 1 に送信する。

【0073】

ユーザホームネットワーク 5 は、受信したサービスプロバイダセキュアコンテナに含まれる取扱方針から使用許諾情報を生成し、使用許諾情報に沿って、コンテンツを利用する。ユーザホームネットワーク 5 において、コンテンツ鍵 K c o が復号されると、課金情報が生成される。課金情報は、所定のタイミングで、暗号化され、取扱方針と共に署名が付され、EMDサービスセンタ 1 に送信される。

【0074】

EMDサービスセンタ 1 は、課金情報および取扱方針を基に使用料金を算出し、また EMDサービスセンタ 1、コンテンツプロバイダ 2、およびサービスプロバイダ 3 それぞれの利益を算出する。EMDサービスセンタ 1 は、さらに、コンテンツプロバイダ 2 から受信した取扱方針、サービスプロバイダ 3 から受信した価格情報、並びにユーザホームネットワーク 5 から受信した課金情報および取扱方針を比較し、サービスプロバイダ 3 またはユーザホームネットワーク 5 で取扱方針の改竄または不正な価格の付加等の不正がなかったか否かを監査する。

【0075】

図 1-3 は、コンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナは、コンテンツ鍵 K c o で暗号化されたコンテンツ、配送用鍵 K d で暗号化されたコンテンツ鍵 K c o、取扱方針、および署名を含む。署名は、コンテンツ鍵 K c o で暗号化されたコンテンツ、配送用鍵 K

dで暗号化されたコンテンツ鍵 K_{co} 、および取扱方針にハッシュ関数を適用して生成されたハッシュ値を、コンテンツプロバイダ2の秘密鍵 K_{scp} で暗号化したデータである。

【0076】

図14は、コンテンツプロバイダ2の証明書を説明する図である。コンテンツプロバイダ2の証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ2に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、コンテンツプロバイダ2の名前、コンテンツプロバイダの公開鍵 K_{cp} 、並びに署名を含む。署名は、証明書のバージョン番号、認証局がコンテンツプロバイダ2に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、コンテンツプロバイダ2の名前、並びにコンテンツプロバイダの公開鍵 K_{cp} にハッシュ関数を適用して生成されたハッシュ値を、認証局の秘密鍵 K_{sca} で暗号化したデータである。

【0077】

図15は、サービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵 K_{co} で暗号化されたコンテンツ、配送用鍵 K_d で暗号化されたコンテンツ鍵 K_{co} 、取扱方針、価格情報、および署名を含む。署名は、コンテンツ鍵 K_{co} で暗号化されたコンテンツ、配送用鍵 K_d で暗号化されたコンテンツ鍵 K_{co} 、取扱方針、および価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ3の秘密鍵 K_{ssp} で暗号化したデータである。

【0078】

図16は、サービスプロバイダ3の証明書を説明する図である。サービスプロバイダ3の証明書は、証明書のバージョン番号、認証局がサービスプロバイダ3に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ3の名前、サービスプロバイダの公開鍵 K_{sp} 、並びに署名を含む。署名は、証明書のバージョン番号、認証局がサービスプロバイダ3に対し割り付ける証明書の通し番号、署名

に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ3の名前、サービスプロバイダの公開鍵 K_{psp} にハッシュ関数を適用して生成されたハッシュ値を、認証局の秘密鍵 K_{sca} で暗号化したデータである。

【0079】

図17は、取扱方針、価格情報、および使用許諾条件情報を示す図である。コンテンツプロバイダ2が有する取扱方針（図17（A））は、コンテンツ毎に用意され、ユーザホームネットワーク5が利用可能な利用内容を示す。例えば、図17（A）の取り扱い方針は、ユーザホームネットワーク5がそのコンテンツを再生およびマルチコピーすることは許可するが、シングルコピーは許可しないことを示す。

【0080】

図18は、シングルコピーおよびマルチコピーを説明する図である。マルチコピーは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合において、そのコンテンツから、複数のコピーを作成することを言う。ただし、図18（A）に示すように、コピーを更にコピーすることはできない（許されない）。シングルコピーは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合において、そのコンテンツから、ただ1つのコピーを作成することを言う。シングルコピーの場合も、図18（B）に示すように、コピーを更にコピーすることはできない（許されない）。

【0081】

サービスプロバイダ3は、図17（B）に示すように、コンテンツプロバイダ2からの取扱方針（図17（A））に価格情報を加える。例えば、図17（B）の価格情報は、そのコンテンツを再生して利用するときの料金が150円で、マルチコピーして利用するときの利用料金が80円であることを示す。図17には、例示しないが、シングルコピーの価格情報は、コピーの1回当たりの使用料金を表し、例えば、3回のコピーの利用では、シングルコピーの使用料金の3倍の料金を支払う。マルチコピーまたはシングルコピーが許可されるコンテンツは、

使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合における、そのコンテンツに限られる。

【0082】

ユーザホームネットワーク5は、サービスプロバイダ3から供給される取扱方針が示すコンテンツの利用可能な利用内容（図17（B））から、ユーザが選択した、利用内容を示す使用許諾条件情報（図17（C））を記憶する。例えば、図17（C）の使用許諾条件情報は、そのコンテンツを再生して使用することができ、シングルコピーおよびマルチコピーができないことを示す。

【0083】

図19は、図17の例と比較してコンテンツプロバイダ2が取扱方針に利益分配の情報を加え、サービスプロバイダ3が価格情報に利益分配の情報を加える場合の、取扱方針および価格情報を説明する図である。図17に示す例に対して、図19の例では、コンテンツプロバイダ2の利益が、コンテンツを再生して利用するとき70円で、マルチコピーして利用するとき40円であることを示す情報が、追加されている（図19（A））。更に、利益分配情報として、サービスプロバイダ3の利益が、コンテンツを再生して利用するとき60円で、マルチコピーして利用するとき30円であることが、追加されている（図19（B））。価格は、図17（A）における場合と同様に、再生が150円、マルチコピーが40円とされている。価格（例えば150円）からコンテンツプロバイダ2の利益（例えば70円）およびサービスプロバイダ3の利益（例えば60円）を差し引いた金額（例えば20円）が、EMDサービスセンタ1の利益である。EMDサービスセンタ1は、ユーザホームネットワーク5のコンテンツの利用結果を示す課金情報（図19（C））とともに、ユーザホームネットワーク5を介して、取扱方針、利益分配率、および価格情報を得ることで、コンテンツプロバイダ2、サービスプロバイダ3、およびEMDサービスセンタ1のそれぞれの利益を算出できる。

【0084】

図20は、コンテンツの再生の利用に、複数の形態が設定されているときの取扱方針、価格情報、および使用許諾条件情報を説明する図である。図20（A）の例では、サービスプロバイダ3において、取扱方針および価格情報として、コ

コンテンツの再生利用に、制限のない再生、回数制限（この例の場合、5回）のある再生、および期日制限（この例の場合、1998年12月31日まで）のある再生が設定されている。ユーザが、5回の回数制限のある再生を選択して、コンテンツを利用する場合、コンテンツを受け取り、まだ1度も再生していない状態では、図20（B）に示すように、ユーザホームネットワーク5の使用許諾条件情報の回数制限に対応する値には、“5”が記録されている。この回数制限に対応する値は、ユーザホームネットワーク5において、コンテンツが再生（利用）される度にデクリメントされ、例えば、3回再生された後、その値は、図20（C）に示すように“2”とされる。回数制限に対応する値が、“0”となった場合、ユーザホームネットワーク5は、それ以上、そのコンテンツを再生して利用することができない。

【0085】

図21は、EMDサービスセンタ1、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の間で送受信される情報の他の例を説明する図である。図12に示した例に対して、図21の例では、サービスプロバイダ3は、コンテンツプロバイダ2からの取扱方針を基に取扱制御情報を作成する。取扱制御情報は、コンテンツなどと共にサービスプロバイダセキュアコンテナに格納され、ユーザホームネットワーク5に送信され、EMDサービスセンタ1にも送信される。取扱制御情報は、更に、課金情報および取扱方針と共にユーザホームネットワーク5からEMDサービスセンタ1に送信される。

【0086】

図22は、図21の例の場合のサービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵K_{co}で暗号化されたコンテンツ、配送用鍵K_dで暗号化されたコンテンツ鍵K_{co}、取扱方針、取扱制御情報、価格情報、および署名を含む。署名は、コンテンツ鍵K_{co}で暗号化されたコンテンツ、配送用鍵K_dで暗号化されたコンテンツ鍵K_{co}、取扱方針、取扱制御情報、および価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ3の秘密鍵K_{ssp}で暗号化したデータである。

【0087】

図23は、図21の例の場合における、取扱方針、取扱制御情報、価格情報、及び使用許諾条件の構成を示す図である。図23に示す例の場合、コンテンツプロバイダ2の取扱方針（図23（A））は、そのまま価格情報を付しても、取扱方針と対比して価格情報を参照できる形式を有しない。そこで、サービスプロバイダ3は、その取扱方針を基に、価格情報と対比して価格情報を参照できる形式を有する取扱制御情報を生成し、それに価格情報を付して、ユーザホームネットワーク5に送信する（図23（B））。ユーザホームネットワークでは、送信を受けた情報から使用許諾条件情報（図23（C））を生成する。図23のコンテンツプロバイダ2は、図12の場合に比較し、より小さいデータ量の取扱方針を記録すればよい利点がある。

【0088】

図24は、EMDサービスセンタ1、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の間で送受信されるコンテンツおよびコンテンツに付随する情報のさらに他の構成を説明する図である。図21に示した例に対して、図24の例では、取扱方針、取扱制御情報、価格情報、および課金情報は、公開鍵暗号により暗号化され、送信される。図24のシステムは、図21の例の場合に比較して、システムの外部からの攻撃に対し、安全性が向上する。

【0089】

図25は、図24の例の場合のコンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナは、コンテンツ鍵K_{co}で暗号化されたコンテンツ、配送用鍵K_dで暗号化されたコンテンツ鍵K_{co}、配送用鍵K_dで暗号化された取扱方針、および署名を含む。署名は、コンテンツ鍵K_{co}で暗号化されたコンテンツ、配送用鍵K_dで暗号化されたコンテンツ鍵K_{co}、および配送用鍵K_dで暗号化された取扱方針にハッシュ関数を適用して生成されたハッシュ値を、コンテンツプロバイダ2の秘密鍵K_{scp}で暗号化したデータである。

【0090】

図26は、図24の例の場合のサービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵K_{co}で暗号化されたコンテンツ、配送用鍵K_dで暗号化されたコンテンツ鍵K_{co}、配送用鍵K_dで暗号化された取扱方針、配送用鍵K_dで暗号化された取扱制御情報、配送用鍵K_dで暗号化された価格情報、および署名を含む。署名は、コンテンツ鍵K_{co}で暗号化されたコンテンツ、配送用鍵K_dで暗号化されたコンテンツ鍵K_{co}、配送用鍵K_dで暗号化された取扱方針、配送用鍵K_dで暗号化された取扱制御情報、および配送用鍵K_dで暗号化された価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ3の秘密鍵K_{ssp}で暗号化したデータである。

【0091】

図27は、EMDサービスセンタ1が、ユーザホームネットワーク5から課金情報を受信するときの動作を説明する図である。ユーザホームネットワーク5と相互認証した後、ユーザ管理部18は、一時鍵K_{temp}を共有化し、鍵サーバ14からの配送用鍵K_dをユーザホームネットワーク5に送信する。ユーザホームネットワーク5は、共有化した一時鍵K_{temp}を用いて課金情報、および取扱方針等を暗号化し、EMDサービスセンタ1に送信する。ユーザ管理部18はこれを受信する。ユーザ管理部18は、受信した課金情報、および取扱方針等を経歴データ管理部15および課金請求部19に送信する。経歴データ管理部15は決済を実行すると判定した場合、受信した課金情報を利益分配部16に送信し、さらに、受信した課金情報および取扱方針等を課金請求部19に送信する。利益分配部16は、コンテンツプロバイダ2、サービスプロバイダ3、およびEMDサービスセンタ1自身に対する請求金額および支払金額を算出する。課金請求部19は、ユーザの支払い金額を算出し、その情報を出納部20に送信する。出納部20は、図示せぬ外部の銀行等と通信し、決算処理を実行する。その際、ユーザの料金の未払い等の情報があれば、それらの情報は、課金請求部19およびユーザ管理部18に送信され、以後のユーザの登録処理時、または配送用鍵K_dの送信処理時に参照される。

【0092】

図28は、EMDサービスセンタ1の利益分配処理の動作を説明する図である。

経歴データ管理部15は、ユーザのコンテンツの使用実績を示す課金情報、取扱方針、および価格データを利益分配部16に送信する。利益分配部16は、これらの情報を基に、コンテンツプロバイダ2、サービスプロバイダ3、およびEMDサービスセンタ1それぞれの利益を算出し、その結果をサービスプロバイダ管理部11、コンテンツプロバイダ管理部12、出納部20、および著作権管理部13に送信する。出納部20は、図示せぬ外部の銀行等と通信し、決算処理を実行する。サービスプロバイダ管理部11は、サービスプロバイダ3の利益の情報をサービスプロバイダ3に送信する。コンテンツプロバイダ管理部12は、コンテンツプロバイダ2の利益の情報をコンテンツプロバイダ2に送信する。監査部21は、ユーザホームネットワーク5の機器から供給された課金情報、価格情報、および取扱方針の正当性を監査する。

【0093】

図29は、EMDサービスセンタ1の、コンテンツの利用実績の情報をJASRACに送信する処理の動作を説明する図である。経歴データ管理部15は、ユーザのコンテンツの使用実績を示す課金情報を著作権管理部13および利益分配部16に送信する。利益分配部16は、JASRACに対する請求金額および支払金額を算出し、その情報を出納部20に送信する。出納部20は、図示せぬ外部の銀行等と通信し、決算処理を実行する。著作権管理部13は、ユーザのコンテンツの使用実績をJASRACに送信する。

【0094】

次に、供給された、暗号化されているコンテンツをメモリスティックに記憶させ、不正の防止を図りつつ、そのコンテンツを他の再生装置などで利用できるようにしたユーザホームネットワーク5の実施の形態の構成を図30に示す。図10の場合と同様の部分には、同一の番号を付してあり、その説明は適宜省略する。なお、図30において、ICカードインターフェース64およびICカード55の図示を省略する。

【0095】

レシーバ51に装着され、コンテンツを記憶するメモリスティック111は、コンテンツ等の記憶等を制御する制御ブロック121および実際にコンテンツ等を記憶する情報記憶ブロック122からなる。制御ブロック121は、シングルチップの暗号処理専用ICで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出せない耐タンパー性を有する。

【0096】

制御ブロック121は、通信部121、メモリコントローラ132、相互認証部133、暗号化部134、記憶部135、復号部136、乱数生成部137、およびデータ検査部138からなる。通信部131は、レシーバ51からコンテンツまたは暗号化されたコンテンツ鍵Kc0等を受信し、レシーバ51にコンテンツまたは暗号化されたコンテンツ鍵Kc0などを送信する。メモリコントローラ132は、通信部131が受信した暗号化されたコンテンツまたはコンテンツ鍵Kc0等を、情報記憶ブロック122に書き込み、また、情報記憶ブロック122に書き込まれたコンテンツ等を読み出し、通信部131等へ供給する。相互認証部133は、レシーバ51の相互認証モジュール71と、相互認証処理により、相互認証し、相互認証後、レシーバ51との通信で、所定の期間利用される一時鍵Ktempを生成する。

【0097】

暗号化部134は、一旦、復号部136が復号したコンテンツ鍵Kc0を、保存用鍵Ksaveで暗号化し、メモリコントローラ132へ供給する。復号部136は、一時鍵Ktempで暗号化されたコンテンツ鍵Kc0、または保存用鍵Ksaveで暗号化されたコンテンツ鍵Kc0などを復号し、暗号化部134または通信部131へ供給する。記憶部135は、そのメモリスティック111に固有の（メモリスティック111毎に、異なる）値を有する保存用鍵Ksaveおよび検査用鍵Kchなどを記憶し、暗号化部134または復号部136へ供給する。記憶部135の記憶の態様については、図36および図38で詳細に説明する。

【0098】

乱数生成部137は、後述する情報記憶ブロック122に記憶されている平文（暗号化されていない）のコンテンツを、メモリスティック111内部で暗号化するときに必要な鍵である、所定の桁数の乱数を生成する。データ検査部138は、記憶部135に記憶されている所定の検査値（検査用のデータ）と後述する鍵データ143に記憶されている所定のデータのハッシュ値とを比較することにより、情報記憶ブロック122に記憶されている記憶されているコンテンツ鍵Kc oおよび使用許諾条件情報などが改竄されていないか否かを検査する。データ検査部138は、また、情報記憶ブロック122に記憶されているコンテンツの移動または情報記憶ブロック122へのコンテンツの書き込みのとき、所定の検査値を生成し、記憶部135に記憶させる。

【0099】

情報記憶ブロック122は、EEPROM(Electrically Erasable Programmable Read Only Memory)、フラッシュメモリ、強誘電体メモリなどの電氣的に記憶内容を書き換えできる、汎用の不揮発性メモリで構成され、データ検索性テーブル141、識別情報142、鍵データ143、暗号化データ144、および非暗号化データ145が記憶される。データ検索性テーブル141には、鍵データ143、暗号化データ144、および非暗号化データ145として記憶されている情報の内容とその記憶位置を表すデータが記憶されている。識別情報142には、記憶されている情報の内容が、暗号化されているか否かを示すデータが記憶される。鍵データ143としては、暗号化データ144に記憶されているコンテンツ毎に、コンテンツ鍵Kc o、コンテンツID、および使用許諾条件情報が記憶されている。鍵データ143の記憶の態様については、図35および図37で詳細に説明する。暗号化データ144としては、暗号化されたコンテンツが記憶されている。非暗号化データ145としては、暗号化されていない、コンテンツの使用許諾情報等が記憶される。

【0100】

図30のレシーバ51は、図10のレシーバ51に、メモリスティックインターフェース112および外部記憶部133が追加されている構成を有する。メモ

リスティックインターフェース 112 は、SAM 62 からの信号を所定の形式に変更し、レシーバ 51 に装着されたメモリスティック 111 に出力し、また、メモリスティック 111 からの信号を所定の形式に変更し、SAM 62 に出力する。外部記憶部 113 は、汎用の不揮発性メモリで構成され、SAM 62 から供給されたコンテンツ鍵 K c o などを記憶し、記憶しているコンテンツ鍵 K c o などを SAM 62 に出力するようになされている。外部記憶部 113 の記憶の態様については、図 31 および図 33 で詳細に説明する。

【0101】

更に、図 30 の SAM 62 は、図 10 の SAM 62 データ検査モジュール 114 を有する。データ検査モジュール 114 は、記憶モジュール 73 に記憶されている所定の検査データと外部記憶部 113 が記憶する所定のデータのハッシュ値を比較することにより、外部記憶部 113 に記憶されている記憶されているコンテンツ鍵 K c o および使用許諾条件情報などが改竄されていないか否かを検査する。データ検査モジュール 114 は、また、HDD 52 に記憶されているコンテンツの移動または HDD 52 へのコンテンツの書き込みのとき、所定の検査値を生成し、記憶モジュール 73 に記憶させる。

【0102】

外部記憶部 113 の記憶の態様について、図 31 を参照して説明する。外部記憶部 113 の記憶領域は、所定の数の鍵データブロックに分割されている（図 31 では、5 つの鍵データブロックに分割されている）。それぞれの鍵データブロックは、例えば、2 組のコンテンツ鍵 K c o、コンテンツ ID、および使用許諾条件情報を記憶できる。鍵データブロックに記憶されている 1 組のコンテンツ鍵 K c o、コンテンツ ID、および使用許諾条件情報は、コンテンツ ID で特定される HDD 52 に記憶されているコンテンツに対応している。鍵データブロック 4 の前半部分に記憶されていたコンテンツ鍵 K c o、コンテンツ ID、および使用許諾条件情報に対応するコンテンツが、HDD 52 から、メモリスティック 111 に移動したとき、鍵データブロック 4 の前半部分に記憶されていたコンテンツ鍵 K c o、コンテンツ ID、および使用許諾条件情報は、消去され、図 31 に示すように、鍵データブロック 4 の前半部分にコンテンツ鍵 K c o 等が記憶されていない部分が

生じる。同様の操作で、図31の鍵データブロック3の後半部分もコンテンツ鍵Kc o等が記憶されていない。

【0103】

図32は、ユーザホームネットワーク5が、図30に示す構成を有するときの、記憶モジュール73の記憶の態様を説明する図である。図32の記憶モジュール73は、ユーザの秘密鍵K s u、課金情報、保存用鍵K s a v e、および配送用鍵K dに加えて、図31で説明した、外部記憶部113の鍵データブロックに対応する検査値を記憶する。例えば、記憶モジュール73の検査値1は、データ検査モジュール114が、外部記憶部113の鍵データブロック1のデータ（すなわち、コンテンツ鍵K c o 1、コンテンツID1、使用許諾条件情報1、コンテンツ鍵K c o 2、コンテンツID2、および使用許諾条件情報2）にハッシュ関数を適用して得られた値であり、同様に、検査値2は、データ検査モジュール114が、鍵データブロック2のデータにハッシュ関数を適用して得られた値である。検査値3、検査値4、および検査値5は、同様に、鍵データブロック3、鍵データブロック4、および鍵データブロック5にそれぞれ対応する。

【0104】

すなわち、例えば、鍵データブロック3にハッシュ関数を適用して得られたハッシュ値と検査値3が一致すれば、鍵データブロック3に記憶されているコンテンツ鍵K c o 5、コンテンツID5、および使用許諾条件情報5は、改竄されていないことがわかる。一方、鍵データブロック3にハッシュ関数を適用して得られたハッシュ値と検査値3が一致しなければ、鍵データブロック3に記憶されているコンテンツ鍵K c o 5、コンテンツID5、および使用許諾条件情報5のいずれかが、改竄されていると判定できる。

【0105】

検査値は、耐タンパー性のあるSAM62の記憶モジュール73に記憶され、外部から不正に読み出すことが困難であるので、改竄が防止され、従って、図30に示すレシーバ51に記憶されたコンテンツ鍵K c oおよびHDD52に記憶されたコンテンツは、不正に対して極めて耐性が高い。

【0106】

図33は、外部記憶部113の他の記憶の態様を説明する図である。図33に示す場合、外部記憶部113は、コンテンツ鍵Kco、コンテンツID、および使用許諾条件情報の組に加えて、鍵データブロックに対応した検査値も記憶する。図33における、例えば、外部記憶部113の検査値1は、データ検査モジュール114が、外部記憶部113の鍵データブロック1のデータ（すなわち、コンテンツ鍵Kco1、コンテンツID1、使用許諾条件情報1、コンテンツ鍵Kco2、コンテンツID2、および使用許諾条件情報2）にハッシュ関数を適用して得られた値を、更に、記憶モジュール73に記憶する、レシーバ51特有の値を有する検査用鍵Kchで暗号化した値である。検査値2、検査値3、検査値4、および検査値5は、同様に、鍵データブロック2、鍵データブロック3、鍵データブロック4、および鍵データブロック5にそれぞれ対応する。

【0107】

図34は、ユーザホームネットワーク5が、図30に示す構成を有し、外部記憶部113が、図33に示す記憶の態様を有するときの、記憶モジュール73の記憶の態様を説明する図である。図34の記憶モジュール73は、レシーバ51（ユーザ）の秘密鍵Ksu、課金情報、保存用鍵Ksave、および配送用鍵Kdに加えて、検査用鍵Kchが記憶されている。

【0108】

すなわち、例えば、外部記憶部113の鍵データブロック3にハッシュ関数を適用して得られたハッシュ値と、外部記憶部113の検査値3を検査用鍵Kdで復号した値が一致すれば、外部記憶部113の鍵データブロック3に記憶されているコンテンツ鍵Kco5、コンテンツID5、および使用許諾条件情報5は、改竄されていないことがわかる。一方、外部記憶部113の鍵データブロック3にハッシュ関数を適用して得られたハッシュ値と、外部記憶部113の検査値3を検査用鍵Kdで復号した値が一致しなければ、外部記憶部113の鍵データブロック3に記憶されているコンテンツ鍵Kco5、コンテンツID5、および使用許諾条件情報5のいずれかが、改竄されていると判定できる。

【0109】

図31および図32に示す場合に比較し、図33に示す外部記憶部113および図34に示す記憶モジュール73は、検査値が耐タンパー性を有するメモリに較べ低価格な汎用メモリに記憶されるので、大量のコンテンツに対応する検査値を記憶できるレシーバ51が、安価に実現できる。

【0110】

次に、鍵データ143の記憶の態様について、図35を参照して説明する。鍵データ143の記憶領域は、所定の数の鍵データブロックに分割されている（図35では、4つの鍵データブロックに分割されている）。それぞれの鍵データブロックは、例えば、2組のコンテンツ鍵Kco、コンテンツID、および使用許諾条件情報を記憶できる。鍵データブロックに記憶されている1組のコンテンツ鍵Kco、コンテンツID、および使用許諾条件情報は、コンテンツIDで特定される暗号化データ144に記憶されているコンテンツに対応している。鍵データブロック3の後半部分に記憶されていたコンテンツ鍵Kco、コンテンツID、および使用許諾条件情報に対応するコンテンツが、メモリスティック111から、HDD52に移動したとき、鍵データブロック4の後半部分に記憶されていたコンテンツ鍵Kco、コンテンツID、および使用許諾条件情報は、消去され、図35に示すように、鍵データブロック4の後半部分にコンテンツ鍵Kco等が記憶されていない部分が生じる。

【0111】

図36は、ユーザホームネットワーク5が、図30に示す構成を有するときの、記憶部135の記憶の態様を説明する図である。記憶部135は、ユーザの秘密鍵Ksu、課金情報、保存用鍵Ksave、および配送用鍵Kdに加えて、図35で説明した、鍵データ143の鍵データブロックに対応する検査値を記憶する。例えば、記憶部135の検査値1は、データ検査部138が、鍵データ143の鍵データブロック1のデータ（すなわち、コンテンツ鍵Kco1、コンテンツID1、使用許諾条件情報1、コンテンツ鍵Kco2、コンテンツID2、および使用許諾条件情報2）にハッシュ関数を適用して得られた値であり、同様に、検査値2は、データ検査部138が、鍵データブロック2のデータにハッシュ関数

を適用して得られた値である。検査値 3 および検査値 4 は、同様に、鍵データブロック 3 および鍵データブロック 4 にそれぞれ対応する。

【0112】

すなわち、例えば、鍵データ 143 の鍵データブロック 3 にハッシュ関数を適用して得られたハッシュ値と記憶部 135 の検査値 3 が一致すれば、鍵データ 143 の鍵データブロック 3 に記憶されているコンテンツ鍵 Kc o 5、コンテンツ ID5、および使用許諾条件情報 5 は、改竄されていないことがわかる。一方、鍵データブロック 3 にハッシュ関数を適用して得られたハッシュ値と検査値 3 が一致しなければ、鍵データブロック 3 に記憶されているコンテンツ鍵 Kc o 5、コンテンツ ID5、および使用許諾条件情報 5 のいずれかが、改竄されていると判定できる。

【0113】

レシーバ 51 のときと同様に、メモリスティック 111 の検査値は、耐タンパ性のある制御ブロック 121 の記憶部 135 に記憶され、外部から不正に読み出すことが困難であるので、改竄が防止され、従って、図 30 に示すメモリスティック 111 に記憶されたコンテンツ鍵 Kc o およびコンテンツは、不正に対して極めて耐性が高い。

【0114】

図 37 は、鍵データ 143 の他の記憶の態様を説明する図である。図 37 に示す場合、鍵データ 143 は、コンテンツ鍵 Kc o、コンテンツ ID、および使用許諾条件情報の組に加えて、鍵データブロックに対応した検査値も記憶する。図 37 における、例えば、鍵データ 143 の検査値 1 は、データ検査部 138 が、鍵データ 143 の鍵データブロック 1 のデータ（すなわち、コンテンツ鍵 Kc o 1、コンテンツ ID1、使用許諾条件情報 1、コンテンツ鍵 Kc o 2、コンテンツ ID2、および使用許諾条件情報 2）にハッシュ関数を適用して得られた値を、更に、~~記憶部 135 に記憶する、メモリスティック 111 特有の値を有する検査用鍵 Kc h~~（従って、レシーバ 51 の記憶モジュール 73 が記憶する検査用鍵 Kc h とは、その値が異なる）で暗号化した値である。検査値 2、検査値 3、および検査値 4 は、同様に、鍵データブロック 2、鍵データブロック 3、および鍵データ

ブロック4にそれぞれ対応する。

【0115】

図38は、ユーザホームネットワーク5が、図30に示す構成を有し、メモリスティック111の鍵データ143が、図37に示す記憶の態様を有するときの、記憶部135の記憶の態様を説明する図である。図38の記憶部135は、メモリスティック111の秘密鍵K_{su}2、および保存用鍵K_{save}に加えて、検査用鍵K_{ch}が記憶されている。

【0116】

すなわち、例えば、鍵データ143の鍵データブロック3にハッシュ関数を適用して得られたハッシュ値と、鍵データ143の検査値3を検査用鍵K_dで復号した値が一致すれば、鍵データ143の鍵データブロック3に記憶されているコンテンツ鍵K_{co}5、コンテンツID5、および使用許諾条件情報5は、改竄されていないことがわかる。一方、鍵データ143の鍵データブロック3にハッシュ関数を適用して得られたハッシュ値と鍵データ143の検査値3を検査用鍵K_dで復号した値が一致しなければ、鍵データ143の鍵データブロック3に記憶されているコンテンツ鍵K_{co}5、コンテンツID5、および使用許諾条件情報5のいずれかが、改竄されていると判定できる。

【0117】

図37に示す鍵データ143および図38に示す記憶部135は、検査値が耐タンパー性を有するメモリに較べ低価格な汎用メモリに記憶されるので、大量のコンテンツに対応する検査値を記憶できるスティックメモリ111が、安価に実現できる。

【0118】

次に、EMDシステムの処理について説明する。図39は、このシステムのコンテンツの配布および再生の処理を説明するフローチャートである。ステップS11において、EMDサービスセンタ1のコンテンツプロバイダ管理部12は、コンテンツプロバイダ2に配送用鍵K_dを送信し、コンテンツプロバイダ2がこれを受信する。その処理の詳細は、図41のフローチャートを参照して後述する。ステップS12において、ユーザは、ユーザホームネットワーク5の機器（例えば

、図10のレシーバ51)を操作し、ユーザホームネットワーク5の機器をEMDサービスセンタ1のユーザ管理部18に登録する。この登録処理の詳細は、図45のフローチャートを参照して後述する。ステップS13において、EMDサービスセンタ1のユーザ管理部18は、ユーザホームネットワーク5と、図42乃至図44に示したように相互認証した後、ユーザホームネットワーク5の機器に、配送用鍵Kdを送信する。ユーザホームネットワーク5はこの鍵を受信する。この処理の詳細は、図53のフローチャートを参照して説明する。

【0119】

ステップS14において、コンテンツプロバイダ2のセキュアコンテナ作成部38は、サービスプロバイダ3にコンテンツプロバイダセキュアコンテナを送信する。この送信処理の詳細は、図55のフローチャートを参照して後述する。ステップS15において、サービスプロバイダ3のセキュアコンテナ作成部44は、ユーザホームネットワーク5からの要求に応じて、ネットワーク4を介して、ユーザホームネットワーク5にサービスプロバイダセキュアコンテナを送信する。この送信処理の詳細は、図57のフローチャートを参照して後述する。ステップS16において、ユーザホームネットワーク5の課金モジュール72は、課金処理を実行する。課金処理の詳細は、図59のフローチャートを参照して後述する。ステップS17において、ユーザは、ユーザホームネットワーク5の機器でコンテンツを再生する。再生処理の詳細は、図63のフローチャートを参照して後述する。

【0120】

一方、コンテンツプロバイダ2が、取扱方針を暗号化して送信する場合の処理は、図40のフローチャートで示すようになる。ステップS21において、EMDサービスセンタ1のコンテンツプロバイダ管理部12は、コンテンツプロバイダ2に配送用鍵Kdを送信する。ステップS22において、EMDサービスセンタ1のサービスプロバイダ管理部11は、サービスプロバイダ3に配送用鍵Kdを送信する。それ以降のステップS23乃至ステップS28の処理は、図39のステップS12乃至ステップS17の処理と同様の処理であり、その説明は省略する。

【0121】

図41は、図39のステップS11および図40のステップS21に対応する、EMDサービスセンタ1がコンテンツプロバイダ2へ配送用鍵Kdを送信し、コンテンツプロバイダ2がこれを受信する処理の詳細を説明するフローチャートである。ステップS31において、EMDサービスセンタ1の相互認証部17は、コンテンツプロバイダ2の相互認証部39と相互認証する。この相互認証処理の詳細は、図42を参照して後述する。相互認証処理により、コンテンツプロバイダ2が、正当なプロバイダであることが確認されたとき、ステップS32において、コンテンツプロバイダ2の暗号化部34および暗号化部36は、EMDサービスセンタ1のコンテンツプロバイダ管理部12から送信された配送用鍵Kdを受信する。ステップS33において、コンテンツプロバイダ2の暗号化部34は、受信した配送用鍵Kdを記憶する。

【0122】

このように、コンテンツプロバイダ2は、EMDサービスセンタ1から配送用鍵Kdを受け取る。同様に、図40に示すフローチャートの処理を行う例の場合、コンテンツプロバイダ2以外に、サービスプロバイダ3も、図41と同様の処理で、EMDサービスセンタ1から配送用鍵Kdを受け取る。

【0123】

次に、図41のステップS31における、いわゆるなりすましがいないことを確認する相互認証の処理について、1つの共通鍵を用いる（図42）、2つの共通鍵を用いる（図43）、および公開鍵暗号を用いる（図44）を例として説明する。

【0124】

図42は、1つの共通鍵で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS41において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数R1を生成する（乱数生成部35が生成するようにしてもよい）。ステップS42において、コンテンツプロバイダ2の相互認証部39は、DESを用いて乱数R1を、予め記憶している

共通鍵 K_c で暗号化する（暗号化部 36 で暗号化するようにしてもよい）。ステップ S43 において、コンテンツプロバイダ 2 の相互認証部 39 は、暗号化された乱数 R_1 を EMD サービスセンタ 1 の相互認証部 17 に送信する。

【0125】

ステップ S44 において、EMD サービスセンタ 1 の相互認証部 17 は、受信した乱数 R_1 を予め記憶している共通鍵 K_c で復号する。ステップ S45 において、EMD サービスセンタ 1 の相互認証部 17 は、32ビットの乱数 R_2 を生成する。ステップ S46 において、EMD サービスセンタ 1 の相互認証部 17 は、復号した 64ビットの乱数 R_1 の下位 32ビットを乱数 R_2 で入れ替え、接続 $R_1_H \parallel R_2$ を生成する。なお、ここで R_i_H は、 R_i の上位ビットを表し、 $A \parallel B$ は、 A と B の接続（ n ビットの A の下位に、 m ビットの B を結合して、 $(n+m)$ ビットとしたもの）を表す。ステップ S47 において、EMD サービスセンタ 1 の相互認証部 17 は、DES を用いて $R_1_H \parallel R_2$ を共通鍵 K_c で暗号化する。ステップ S48 において、EMD サービスセンタ 1 の相互認証部 17 は、暗号化した $R_1_H \parallel R_2$ をコンテンツプロバイダ 2 に送信する。

【0126】

ステップ S49 において、コンテンツプロバイダ 2 の相互認証部 39 は、受信した $R_1_H \parallel R_2$ を共通鍵 K_c で復号する。ステップ S50 において、コンテンツプロバイダ 2 の相互認証部 39 は、復号した $R_1_H \parallel R_2$ の上位 32ビット R_1_H を調べ、ステップ S41 で生成した、乱数 R_1 の上位 32ビット R_1_H と一致すれば、EMD サービスセンタ 1 が正当なセンタであることを認証する。生成した乱数 R_1_H と、受信した R_1_H が一致しないとき、処理は終了される。両者が一致するとき、ステップ S51 において、コンテンツプロバイダ 2 の相互認証部 39 は、32ビットの乱数 R_3 を生成する。ステップ S52 において、コンテンツプロバイダ 2 の相互認証部 39 は、受信し、復号した 32ビットの乱数 R_2 を上位に設定し、生成した乱数 R_3 をその下位に設定し、~~接続 $R_2 \parallel R_3$ とする。~~ ステップ S53 において、コンテンツプロバイダ 2 の相互認証部 39 は、DES を用いて ~~接続 $R_2 \parallel R_3$ を共通鍵 K_c で暗号化する。~~ ステップ S54 において、コンテンツプロバイダ 2 の相互認証部 39 は、暗号化された ~~接続 $R_2 \parallel R_3$ を EMD サービス~~

センタ 1 の相互認証部 17 に送信する。

【0127】

ステップ S55 において、EMD サービスセンタ 1 の相互認証部 17 は、受信した接続 R2 || R3 を共通鍵 Kc で復号する。ステップ S56 において、EMD サービスセンタ 1 の相互認証部 17 は、復号した接続 R2 || R3 の上位 32 ビットを調べ、乱数 R2 と一致すれば、コンテンツプロバイダ 2 を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

【0128】

図 43 は、2 つの共通鍵 Kc1, Kc2 で、共通鍵暗号である DES を用いる、コンテンツプロバイダ 2 の相互認証部 39 と EMD サービスセンタ 1 の相互認証部 17 との相互認証の動作を説明するフローチャートである。ステップ S61 において、コンテンツプロバイダ 2 の相互認証部 39 は、64 ビットの乱数 R1 を生成する。ステップ S62 において、コンテンツプロバイダ 2 の相互認証部 39 は、DES を用いて乱数 R1 を予め記憶している共通鍵 Kc1 で暗号化する。ステップ S63 において、コンテンツプロバイダ 2 の相互認証部 39 は、暗号化された乱数 R1 を EMD サービスセンタ 1 に送信する。

【0129】

ステップ S64 において、EMD サービスセンタ 1 の相互認証部 17 は、受信した乱数 R1 を予め記憶している共通鍵 Kc1 で復号する。ステップ S65 において、EMD サービスセンタ 1 の相互認証部 17 は、乱数 R1 を予め記憶している共通鍵 Kc2 で暗号化する。ステップ S66 において、EMD サービスセンタ 1 の相互認証部 17 は、64 ビットの乱数 R2 を生成する。ステップ S67 において、EMD サービスセンタ 1 の相互認証部 17 は、乱数 R2 を共通鍵 Kc2 で暗号化する。ステップ S68 において、EMD サービスセンタ 1 の相互認証部 17 は、暗号化された乱数 R1 および乱数 R2 をコンテンツプロバイダ 2 の相互認証部 39 に送信する。

【0130】

ステップ S69 において、コンテンツプロバイダ 2 の相互認証部 39 は、受信した乱数 R1 および乱数 R2 を予め記憶している共通鍵 Kc2 で復号する。ステ

ップS70において、コンテンツプロバイダ2の相互認証部39は、復号した乱数R1を調べ、ステップS61で生成した乱数R1（暗号化する前の乱数R1）と一致すれば、EMDサービスセンタ1を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップS71において、コンテンツプロバイダ2の相互認証部39は、復号して得た乱数R2を共通鍵Kc1で暗号化する。ステップS72において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数R2をEMDサービスセンタ1に送信する。

【0131】

ステップS73において、EMDサービスセンタ1の相互認証部17は、受信した乱数R2を共通鍵Kc1で復号する。ステップS74において、EMDサービスセンタ1の相互認証部17は、復号した乱数R2が、ステップS66で生成した乱数R2（暗号化する前の乱数R2）と一致すれば、コンテンツプロバイダ2を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

【0132】

図44は、公開鍵暗号である、160ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS81において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数R1を生成する。ステップS82において、コンテンツプロバイダ2の相互認証部39は、自分自身の公開鍵Kpcpを含む証明書（認証局から予め取得しておいたもの）と、乱数R1をEMDサービスセンタ1の相互認証部17に送信する。

【0133】

ステップS83において、EMDサービスセンタ1の相互認証部17は、受信した証明書の署名（認証局の秘密鍵Kscaで暗号化されている）を、予め取得しておいた認証局の公開鍵Kpcaで復号し、コンテンツプロバイダ2の公開鍵Kpcpとコンテンツプロバイダ2の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ2の公開鍵Kpcpおよびコンテンツプロバイダ2の名前を取り出す。証明書が認証局が発行した適正なも

のであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵 K_{pcp} およびコンテンツプロバイダ 2 の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ 2 の公開鍵 K_{pcp} およびコンテンツプロバイダ 2 の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵 K_{pcp} が改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

【0134】

適正な認証結果が得られたとき、ステップ S 8 4 において、EMD サービスセンタ 1 の相互認証部 1 7 は、64 ビットの乱数 R_2 を生成する。ステップ S 8 5 において、EMD サービスセンタ 1 の相互認証部 1 7 は、乱数 R_1 および乱数 R_2 の接続 $R_1 \parallel R_2$ を生成する。ステップ S 8 6 において、EMD サービスセンタ 1 の相互認証部 1 7 は、接続 $R_1 \parallel R_2$ を自分自身の秘密鍵 K_{sec} で暗号化する。ステップ S 8 7 において、EMD サービスセンタ 1 の相互認証部 1 7 は、接続 $R_1 \parallel R_2$ を、ステップ S 8 3 で取得したコンテンツプロバイダ 2 の公開鍵 K_{pcp} で暗号化する。ステップ S 8 8 において、EMD サービスセンタ 1 の相互認証部 1 7 は、秘密鍵 K_{sec} で暗号化された接続 $R_1 \parallel R_2$ 、公開鍵 K_{pcp} で暗号化された接続 $R_1 \parallel R_2$ 、および自分自身の公開鍵 K_{pec} を含む証明書（認証局から予め取得しておいたもの）をコンテンツプロバイダ 2 の相互認証部 3 9 に送信する。

【0135】

ステップ S 8 9 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、受信した証明書の署名を予め取得しておいた認証局の公開鍵 K_{pca} で復号し、正しければ証明書から公開鍵 K_{pec} を取り出す。この場合の処理は、ステップ S 8 3 における場合と同様であるので、その説明は省略する。ステップ S 9 0 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、EMD サービスセンタ 1 の秘密鍵 K_{sec} で暗号化されている接続 $R_1 \parallel R_2$ を、ステップ S 8 9 で取得した公開鍵 K_{pec} で復号する。ステップ S 9 1 において、コンテンツプロバイ

ダ2の相互認証部39は、自分自身の公開鍵 $K_{p\ c\ p}$ で暗号化されている接続 $R_1 \parallel R_2$ を、自分自身の秘密鍵 $K_{s\ c\ p}$ で復号する。ステップS92において、コンテンツプロバイダ2の相互認証部39は、ステップS90で復号された接続 $R_1 \parallel R_2$ と、ステップS91で復号された接続 $R_1 \parallel R_2$ を比較し、一致すればEMDサービスセンタ1を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

【0136】

適正な認証結果が得られたとき、ステップS93において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数 R_3 を生成する。ステップS94において、コンテンツプロバイダ2の相互認証部39は、ステップS90で取得した乱数 R_2 および生成した乱数 R_3 の接続 $R_2 \parallel R_3$ を生成する。ステップS95において、コンテンツプロバイダ2の相互認証部39は、接続 $R_2 \parallel R_3$ を、ステップS89で取得した公開鍵 $K_{p\ e\ s\ c}$ で暗号化する。ステップS96において、コンテンツプロバイダ2の相互認証部39は、暗号化した接続 $R_2 \parallel R_3$ をEMDサービスセンタ1の相互認証部17に送信する。

【0137】

ステップS97において、EMDサービスセンタ1の相互認証部17は、暗号化された接続 $R_2 \parallel R_3$ を自分自身の秘密鍵 $K_{s\ e\ s\ c}$ で復号する。ステップS98において、EMDサービスセンタ1の相互認証部17は、復号した乱数 R_2 が、ステップS84で生成した乱数 R_2 （暗号化する前の乱数 R_2 ）と一致すれば、コンテンツプロバイダ2を適正なプロバイダとして認証し、一致しなければ、不適正なプロバイダとして、処理を終了する。

【0138】

以上のように、EMDサービスセンタ1の相互認証部17とコンテンツプロバイダ2の相互認証部39は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵 $K_{t\ e\ m\ p}$ として利用される。

【0139】

図45は、図39のステップS12および図40のステップS23に対応する、レシーバ51がEMDサービスセンタ1のユーザ管理部18に登録する処理を説

明するフローチャートである。ステップS101において、レシーバ51のSAM62は、ICカードインターフェース64の出力から、レシーバ51にバックアップ用のICカード55が装着されているか否かを判定し、バックアップ用のICカード55が装着されていると判定された場合（例えば、レシーバ51が新たなレシーバ51に変更され、元のレシーバ51のデータを、新たなレシーバ51に引き継ぐために、元のレシーバ51のデータをバックアップ用のICカード55にバックアップさせている場合）、ステップS102に進み、ICカード55に記憶されているバックアップデータの読み込み処理を実行する。この処理の詳細は、図50のフローチャートを参照して後述する。勿論、この読み込み処理が実行されるためには、その前に、ICカード55に、バックアップデータを記憶させる必要があるが、その処理は、図48を参照して後述する。

【0140】

ステップS101において、バックアップ用のICカード55が装着されていないと判定された場合、手続は、ステップS102をスキップし、ステップS103に進む。ステップS103において、SAM62の相互認証モジュール71は、EMDサービスセンタ1の相互認証部17と相互認証し、SAM62は、証明書をEMDサービスセンタ1のユーザ管理部18に送信する。この認証処理は、図42乃至図44を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS103で、SAM62がEMDサービスセンタ1のユーザ管理部18に送信する署名書は、図46に示すデータを含む。SAM62が送信する証明書は、図14に示すコンテンツプロバイダ2の証明書とほぼ同様の構成を有するが、更に、他のSAMに従属するか否かを示すデータを含んでいる。ステップS104において、SAM62は、通信部61を介して、一時鍵Ktempで暗号化した、ユーザの銀行等の決済機関の情報等をEMDサービスセンタ1のユーザ管理部18に送信する。

【0141】

ステップS105において、EMDサービスセンタ1のユーザ管理部18は、受信したSAM62のIDを基に、図7に示したユーザ登録データベースを検索する。ステップS106において、EMDサービスセンタ1のユーザ管理部18は、受信したIDを有するSAM62の登録が可能であるか否かを判定し、受信したIDを有す

るSAM 6 2の登録が可能であると判定された場合、ステップS 1 0 7に進み、受信したIDを有するSAM 6 2が、新規登録であるか否かを判定する。ステップS 1 0 7において、受信したIDを有するSAM 6 2が、新規登録ではないと判定された場合、手続は、ステップS 1 0 8に進む。

【0142】

ステップS 1 0 8において、EMDサービスセンタ1のユーザ管理部18は、更新登録を実行し、受信したIDを基にユーザ登録データベースを検索し、登録リストを作成する。この登録リストは、例えば、図47に示す構造を有し、機器のSAMのIDに対応して、EMDサービスセンタ1のユーザ管理部18が登録を拒絶したか否かを示す登録拒絶フラグ、従属する機器である場合のコンテンツ鍵K c oの利用条件を示すステータスフラグ、従属する機器であるか否かを示すコンディションフラグ、並びに登録拒絶フラグ、ステータスフラグ、およびコンディションフラグにハッシュ関数を適用して生成したハッシュ値をEMDサービスセンタ1の秘密鍵K s e s cで暗号化した署名から構成される。

【0143】

機器のSAMのIDは、機器の固有の64ビットからなるIDを示す（図47では、16進数で示す）。登録拒絶フラグの”1”は、EMDサービスセンタ1のユーザ管理部18が対応するIDを有する機器を登録したことを示し、登録拒絶フラグの”0”は、MDサービスセンタ1のユーザ管理部18が対応するIDを有する機器の登録を拒絶したことを示す。

【0144】

ステータスフラグのMSB(Most Significant Bit)の”1”は、対応するIDを有する子の機器（例えばレコーダ53）が従属した親の機器（例えばレシーバ51）からコンテンツ鍵K c oをもらえることを示し、ステータスフラグのMSBの”0”は、対応するIDを有する子の機器が従属した親の機器からコンテンツ鍵K c oをもらえないことを示している。ステータスフラグの上位から2ビット目の”1”は、対応するIDを有する子の機器が従属した親の機器から、親の機器の保存用鍵K s a v eで暗号化されたコンテンツ鍵K c oをもらえることを示す。ステータスフラグの上位から3ビット目の”1”は、対応するIDを有する子の機器が

従属した親の機器から、配送用鍵 K d で暗号化されたコンテンツ鍵 K c o をもらえることを示す。ステータスフラグの LSB (Least Significant Bit) の ” 1 ” は、従属した親の機器が配送用鍵 K d で暗号化したコンテンツ鍵 K c o を購入し、対応する ID を有する子の機器に、一時鍵 K t e m p で暗号化してコンテンツ鍵 K c o を渡すことを示す。

【 0 1 4 5 】

コンディションフラグの ” 0 ” は、対応する ID を有する機器が EMD サービスセンタ 1 のユーザ管理部 1 8 と直接通信が出来る（すなわち、例えばレシーバ 5 1 のような親の機器である）ことを示し、コンディションフラグの ” 1 ” は、対応する ID を有する機器が EMD サービスセンタ 1 のユーザ管理部 1 8 と直接通信が出来ない（すなわち、例えばレコーダ 5 3 のような子の機器である）ことを示す。コンディションフラグが ” 0 ” のとき、ステータスフラグは常に ” 0 0 0 0 ” に設定される。

【 0 1 4 6 】

ステップ S 1 0 9 において、EMD サービスセンタ 1 のユーザ管理部 1 8 は、相互認証部 1 7 から供給された一時鍵 K t e m p で暗号化した、鍵サーバ 1 4 から供給された配送用鍵 K d をレシーバ 5 1 の SAM 6 2 に送信する。ステップ S 1 1 0 において、レシーバ 5 1 の SAM 6 2 は、受信した配送用鍵 K d を一時鍵 K t e m p で復号し、記憶モジュール 7 3 に記憶させる。

【 0 1 4 7 】

ステップ S 1 1 1 において、EMD サービスセンタ 1 のユーザ管理部 1 8 は、一時鍵 K t e m p で暗号化した登録リストをレシーバ 5 1 の SAM 6 2 に送信する。ステップ S 1 1 2 において、レシーバ 5 1 の SAM 6 2 は、受信した登録リストを一時鍵 K t e m p で復号し、記憶モジュール 7 3 に記憶させ、処理は終了する。

【 0 1 4 8 】

ステップ S 1 0 7 において、受信した ID を有する SAM 6 2 が、新規登録であると判定された場合、手続は、ステップ S 1 1 4 に進み、EMD サービスセンタ 1 のユーザ管理部 1 8 は、新規登録を実行し、登録リストを作成し、ステップ S 1 0 9 に進む。

【0149】

ステップS106において、受信したIDを有するSAM62の登録が不可であると判定された場合、ステップS113に進み、EMDサービスセンタ1のユーザ管理部18は、登録拒絶の登録リストを作成し、ステップS111に進む。

【0150】

このように、レシーバ51は、EMDサービスセンタ1に登録される。

【0151】

次に、今まで使用していたレシーバ51の記憶モジュール73に記憶された配送鍵Kdなどの所定のデータをICカード55に記憶させる処理の詳細を、図48のフローチャートを参照して説明する。ステップS121において、SAM62の相互認証モジュール71は、ICカード55の相互認証モジュール80と相互認証する。この認証処理は、図42乃至図44を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS122において、SAM62の乱数発生ユニット92は、バックアップ鍵Kicとして用いられる乱数を生成する。ステップS123において、SAM62の暗号化ユニット93は、記憶モジュール73に記憶されているSAMのID番号、保存用鍵Ksave、およびHDD52のIDを、バックアップ鍵Kicを用いて暗号化する。ステップS124において、SAM62の暗号化ユニット93は、EMDサービスセンタ1の公開鍵Kpescでバックアップ鍵Kicを暗号化する（SAM62は、EMDサービスセンタ1との間の認証処理（図44のステップS89）において、EMDサービスセンタ1の公開鍵Kpescを取得している）。ステップS125において、レシーバ51のSAM62は、ICカードインターフェース64を介して、暗号化されたSAMのID番号、保存用鍵Ksave、およびHDD52のID並びに暗号化されたバックアップ鍵KicをICカード55に送信し、記憶モジュール81に記憶させる。

【0152】

以上のように、SAM62の記憶モジュール73に記憶されたSAMのID番号、保存用鍵Ksave、およびHDD52のIDは、バックアップ鍵Kicを用いて暗号化され、EMDサービスセンタ1の公開鍵Kpescを用いて暗号化されたバックアップ鍵Kicと共に、ICカード55の記憶モジュール81に記憶される。

【0153】

今まで使用していたレシーバ51の記憶モジュール73に記憶された配送用鍵K_dなどの所定のデータをICカード55に記憶させる他の処理の例の詳細を、図49のフローチャートを参照して説明する。ステップS131において、SAM62の相互認証モジュール71は、ICカード55の相互認証モジュール80と相互認証する。ステップS132において、SAM62の暗号化ユニット93は、記憶モジュール73に記憶されているSAMのID番号、保存用鍵K_{save}、およびHDD52のIDを、EMDサービスセンタ1の公開鍵K_{psc}を用いて暗号化する。ステップS133において、レシーバ51のSAM62は、ICカードインターフェース64を介して、暗号化されたSAMのID番号、保存用鍵K_{save}、およびHDD52のIDをICカード55に送信し、記憶モジュール81に記憶させる。

【0154】

図49に示す処理により、図48に示した場合より簡単な処理で、EMDサービスセンタ1の公開鍵K_{psc}を用いて暗号化されたSAMのID番号、保存用鍵K_{save}、およびHDD52のIDは、ICカード55の記憶モジュール81に記憶される。

【0155】

このように、ICカード55にバックアップされたデータは、図45のステップS102の処理で、新しいレシーバ51に読み込まれる。図50は、図48に示す処理でバックアップされたデータ読み出す場合の処理を説明するフローチャートである。ステップS141において、新しいレシーバ51のSAM62の相互認証モジュール71は、ICカード55の相互認証モジュール80と相互認証する。この認証処理は、図42乃至図44を参照して説明した場合と同様であるので、ここでは説明を省略する。

【0156】

ステップS142において、SAM62は、ICカードインターフェース64を介して、記憶モジュール81に記憶された、バックアップ鍵K_{ic}で暗号化されている古いレシーバ51の記憶モジュール73のデータ（SAMのID番号、保存用鍵K_{save}、およびHDD52のIDを示すバックアップデータ）、およびEMDサービス

センタ1の公開鍵K p e s cで暗号化されているバックアップ鍵K i cを読み出す。ステップS 1 4 3において、SAM 6 2の相互認証モジュール7 1は、通信部6 1を介して、EMDサービスセンタ1の相互認証部1 7と相互認証する。この認証処理は、図4 2乃至図4 4を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS 1 4 4において、SAM 6 2は、通信部6 1を介して、バックアップ鍵K i cで暗号化されている記憶モジュール7 3のデータ、およびEMDサービスセンタ1の公開鍵K p e s cで暗号化されているバックアップ鍵K i cを、EMDサービスセンタ1のユーザ管理部1 8に送信する。

【0 1 5 7】

ステップS 1 4 5において、EMDサービスセンタ1のユーザ管理部1 8は、受信したバックアップ鍵K i cを自分自身の秘密鍵K s e s cで復号する。ステップS 1 4 6において、EMDサービスセンタ1のユーザ管理部1 8は、受信したバックアップデータを、バックアップ鍵K i cで復号する。ステップS 1 4 7において、EMDサービスセンタ1のユーザ管理部1 8は、復号したバックアップデータを、相互認証部1 7から供給された一時鍵K t e m pで、再度、暗号化する。ステップS 1 4 8において、EMDサービスセンタ1のユーザ管理部1 8は、一時鍵K t e m pで暗号化されたバックアップデータを、レシーバ5 1の通信部6 1に送信する。

【0 1 5 8】

ステップS 1 4 9において、レシーバ5 1の通信部6 1は、EMDサービスセンタ1のユーザ管理部1 8から受信したデータを、SAM 6 2に送信し、SAM 6 2は、そのデータを復号した後、記憶モジュール7 3に記憶させる。ステップS 1 6 0において、EMDサービスセンタ1のユーザ管理部1 8は、ICカード5 5にデータを記憶させた古い装置のSAM 6 2のIDに対応するユーザ登録データベース（図7）のデータを登録不可に設定し、処理を終了する。

【0 1 5 9】

このように、新しいレシーバ5 1は、ICカード5 5のバックアップデータを読み込む。

【0160】

図49に示す処理でバックアップされたデータ読み出す場合の処理を、図51に示すフローチャートを用いて説明する。ステップS161において、新しいレシーバ51のSAM62の相互認証モジュール71は、ICカード55の相互認証モジュール80と相互認証する。この認証処理は、図42乃至図44を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS162において、SAM62は、ICカードインタフェース64を介して、EMDサービスセンタ1の公開鍵K_{p e s c}で暗号化されている古いレシーバ51の記憶モジュール73のデータ（SAMのID番号、保存用鍵K_{s a v e}、およびHDD52のIDを示すバックアップデータ）を読み出す。

【0161】

ステップS163において、SAM62の相互認証モジュール71は、通信部61を介して、EMDサービスセンタ1の相互認証部17と相互認証する。この認証処理は、図42乃至図44を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS164において、SAM62は、通信部61を介して、EMDサービスセンタ1の公開鍵K_{p e s c}で暗号化されている記憶モジュール73のデータを、EMDサービスセンタ1のユーザ管理部18に送信する。

【0162】

ステップS165において、EMDサービスセンタ1のユーザ管理部18は、受信した記憶モジュール73のデータを自分自身の秘密鍵K_{s e s c}で復号する。ステップS166において、EMDサービスセンタ1のユーザ管理部18は、復号したバックアップデータを、相互認証部17から供給された一時鍵K_{t e m p}で、再度、暗号化する。ステップS167において、EMDサービスセンタ1のユーザ管理部18は、一時鍵K_{t e m p}で暗号化されたバックアップデータを、レシーバ51の通信部61に送信する。

【0163】

ステップS168において、レシーバ51の通信部61は、EMDサービスセンタ1のユーザ管理部18から受信したデータを、SAM62に送信し、SAM62は、そのデータを復号した後、記憶モジュール73に記憶させる。ステップS16

9において、EMDサービスセンタ1のユーザ管理部18は、ICカード55にデータを記憶させた古い装置のSAM62のIDに対応するユーザ登録データベース（図7）のデータを登録不可に設定する。

【0164】

このように、図49に示す処理を用いたバックアップの場合、図51に示す処理により、新しいレシーバ51は、ICカード55のバックアップデータを読み込む。

【0165】

レシーバ51は、自分自身を登録する場合（図39のステップS12に対応する処理を実行する場合）、図45のフローチャートに示す処理を実行するが、レシーバ51に従属するレコーダ53をEMDサービスセンタ1に登録する場合、図52のフローチャートに示す処理を実行する。ステップS181において、レシーバ51のSAM62は、記憶モジュール73に記憶された登録リストに、レコーダ53のIDを書き込む。ステップS182において、レシーバ51の相互認証モジュール71は、EMDサービスセンタ1の相互認証部17と相互認証する。この認証処理は、図42乃至図44を参照して説明した場合と同様であるので、ここでは説明を省略する。

【0166】

ステップS183において、EMDサービスセンタ1のユーザ管理部18は、レシーバ51のID（図46に示すSAM62の証明書に含まれるSAM62のID）を基に、ユーザ登録データベースを検索し、レシーバ51が登録不可であるか否かを判定し、レシーバ51が登録不可ではないと判定された場合、ステップS184に進み、レシーバ51のSAM62は、EMDサービスセンタ1のユーザ管理部18に、記憶モジュール73に記憶している配送用鍵Kdのバージョン、課金情報（後述の図59に示すフローチャートのステップS337の処理で記憶される）、および登録リスト、並びにHDD52に記録された取扱方針を一時鍵Kdで暗号化し、通信部61を介して、EMDサービスセンタ1のユーザ管理部18に、記憶モジュール73に記憶している配送用鍵Kdのバージョン、課金情報、および登録リスト、並びにHDD52に記録された取扱方針を送信する。ステップS185において

、EMDサービスセンタ1のユーザ管理部18は、受信したデータを復号した後、課金情報を処理し、図47を参照して説明した、レシーバ51から受信した登録リストのレコーダ53に関する登録拒絶フラグ、およびステータスフラグなどのデータの部分を更新し、レシーバ51に対応するデータに応じた署名を付する。

【0167】

ステップS186において、EMDサービスセンタ1のユーザ管理部18は、レシーバ51が有する配送用鍵Kdのバージョンが最新か否かを判定し、レシーバ51が有する配送用鍵Kdのバージョンが最新であると判定された場合、ステップS187に進み、一時鍵Kdで暗号化した、更新した登録リスト、および課金情報受信メッセージを、レシーバ51に送信し、レシーバ51は、更新した登録リスト、および課金情報受信メッセージを受信し、復号した後、記憶する。ステップS188において、レシーバ51は、記憶モジュール73に記憶された課金情報を消去し、登録リストを、EMDサービスセンタ1のユーザ管理部18からステップS187において受信したものに更新し、ステップS191に進む。

【0168】

ステップS186において、レシーバ51が有する配送用鍵Kdのバージョンが最新のものではないと判定された場合、ステップS189に進み、EMDサービスセンタ1のユーザ管理部18は、一時鍵Kdで暗号化した、最新バージョンの配送用鍵Kd、更新した登録リスト、および課金情報受信メッセージを、レシーバ51に送信し、レシーバ51は、最新バージョンの配送用鍵Kd、更新した登録リスト、および課金情報受信メッセージを受信し、復号した後、記憶する。ステップS190において、レシーバ51は、記憶モジュール73に記憶された課金情報を消去し、登録リストを、EMDサービスセンタ1のユーザ管理部18からステップS189において受信したものに更新し、配送用鍵Kdを最新バージョンのものに更新し、ステップS191に進む。

【0169】

ステップS191において、レシーバ51のSAM62は、更新した登録リストを参照し、レコーダ53が登録不可か否かを判定し、レコーダ53が登録不可でないと判定された場合、ステップS192に進み、レシーバ51とレコーダ53

は相互認証し、一時鍵K t e m pを共有する。この認証処理は、図4 2乃至図4 4を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS 1 9 3において、レコーダ5 3に、一時鍵K dで暗号化した、登録完了メッセージ、および配送用鍵K dを送信し、レコーダ5 3は、登録完了メッセージ、および配送用鍵K dを受信し、復号する。ステップS 1 9 4において、レコーダ5 3は、配送用鍵K dを更新し、処理は終了する。

【0170】

ステップS 1 8 3において、レシーバ5 1が登録不可であると判定された場合、および、ステップS 1 9 1において、レコーダ5 3が登録不可であると判定された場合、処理は終了する。

【0171】

以上のように、レシーバ5 1に従属するレコーダ5 3は、レシーバ5 1を介して、EMDサービスセンタ1に登録される。

【0172】

図5 3は、図3 9のステップS 1 3において、EMDサービスセンタ1がレシーバ5 1に送信した配送用鍵K dを、レシーバ5 1が受け取る処理の詳細を説明するフローチャートである。ステップS 2 0 1において、レシーバ5 1の相互認証モジュール7 1は、EMDサービスセンタ1の相互認証部1 7と相互認証する。この認証処理は、図4 2乃至図4 4を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS 2 0 2において、レシーバ5 1のSAM 6 2は、通信部6 1を介して、EMDサービスセンタ1のユーザ管理部1 8に証明書を送信し、EMDサービスセンタ1のユーザ管理部1 8は、証明書を受信する。ステップS 2 0 3乃至ステップS 2 1 0は、図5 2のステップS 1 8 3乃至ステップS 1 9 0と同様の処理であるのでその説明は省略する。

【0173】

このように、レシーバ5 1は、EMDサービスセンタ1のユーザ管理部1 8から配送用鍵K dを受け取り、レシーバ5 1の課金情報をEMDサービスセンタ1のユーザ管理部1 8に送信する。

【0174】

次に、ユーザネットワーク5が図10または図11の構成を有する場合、レシーバ51に従属するレコーダ53の配送用鍵Kdの受け取り処理（図47に示すステータスフラグが、レコーダ53の配送用鍵Kdの受け取りを許可する値を有する場合）を、図54に示すフローチャートを用いて説明する。ステップS221において、レシーバ51の相互認証モジュール71およびレコーダ53の図示せぬ相互認証モジュールは、相互認証する。この認証処理は、図42乃至図44を参照して説明した場合と同様であるので、ここでは説明を省略する。

【0175】

ステップS222において、レシーバ51は、レシーバ51の記憶モジュール73に記憶する登録リストにレコーダ53のデータが載っているか否かを判定し、レシーバ51の記憶モジュール73に記憶する登録リストにレコーダ53のデータが載っていると判定された場合、ステップS223に進み、レシーバ51の記憶モジュール73に記憶する登録リストを基に、レコーダ53が登録不可であるか否かを判定する。ステップS223において、レコーダ53が登録不可ではないと判定された場合、ステップS224に進み、レコーダ53のSAM66は、レシーバ51のSAM62に、内蔵する記憶モジュールに記憶している配送用鍵Kd（後述する図54のステップS235でレシーバ51から受け取っている）のバージョンおよび課金情報（後述する図59に対応する処理のステップS337に相当する処理で記憶している）を一時鍵Ktempで暗号化して、送信し、レシーバ51のSAM62は、配送用鍵Kdのバージョンおよび課金情報を受信し、復号する。

【0176】

ステップS225において、レシーバ51の相互認証モジュール71は、通信部61を介して、EMDサービスセンタ1の相互認証部17と、相互認証する。この認証処理は、図42乃至図44を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS226において、EMDサービスセンタ1のユーザ管理部18は、レシーバ51のIDを基に、ユーザ登録データベースを検索し、レシーバ51が登録不可であるか否かを判定し、レシーバ51が登録不可では

ないと判定された場合、ステップ S 2 2 7 に進み、レシーバ 5 1 の SAM62 は、通信部 6 1 を介して、EMD サービスセンタ 1 のユーザ管理部 1 8 に、一時鍵 K d で暗号化した、記憶モジュール 7 3 に記憶している配送用鍵 K d のバージョン、課金情報、および登録リスト、HDD 5 2 に記録している取扱方針、並びにレコーダ 5 3 の課金情報を送信する。ステップ S 2 2 8 において、EMD サービスセンタ 1 のユーザ管理部 1 8 は、受信したデータを復号した後、課金情報を処理し、図 4 7 で説明した、レシーバ 5 1 から受信した登録リストのレコーダ 5 3 に関する登録拒絶フラグ、ステータスフラグなどのデータの部分を更新し、レシーバ 5 1 に対応するデータに応じた署名を付する。

【0177】

ステップ S 2 2 9 乃至ステップ S 2 3 4 の処理は、図 5 2 に示すステップ S 1 8 6 乃至ステップ S 1 9 1 とそれぞれ同様であるので、その説明は省略する。

【0178】

ステップ S 2 3 4 において、レシーバ 5 1 の SAM 6 2 は、更新した登録リストを参照し、レコーダ 5 3 が登録不可か否かを判定し、レコーダ 5 3 が登録不可でないと判定された場合、ステップ S 2 3 5 に進み、レコーダ 5 3 に、一時鍵 K d で暗号化した、課金情報受信メッセージ、および配送用鍵 K d を送信し、レコーダ 5 3 は、課金情報受信メッセージ、および配送用鍵 K d を受信し、復号する。ステップ S 2 3 6 において、レコーダ 5 3 の SAM 6 6 は、内蔵する記憶モジュールに記憶している、課金情報を消去し、配送用鍵 K d を最新のバージョンに更新する。

【0179】

ステップ S 2 2 2 において、レシーバ 5 1 の記憶モジュール 7 3 に記憶する登録リストにレコーダ 5 3 のデータが載っていないと判定された場合、ステップ S 2 3 7 に進み、図 5 2 に示したレコーダ 5 3 の登録処理を実行し、ステップ S 2 2 4 に進む。

【0180】

ステップ S 2 2 3 において、レコーダ 5 3 が登録不可であると判定された場合、ステップ S 2 2 6 において、レシーバ 5 1 が登録不可であると判定された場合

、および、ステップ S 2 3 4 において、レコーダ 5 3 が登録不可であると判定された場合、処理は終了する。

【0181】

以上のように、レシーバ 5 1 に従属するレコーダ 5 3 は、レシーバ 5 1 を介して、配送用鍵 K d を受け取る。

【0182】

次に、図 3 9 のステップ S 1 4 に対応する、コンテンツプロバイダ 2 がサービスプロバイダ 3 にコンテンツプロバイダセキュアコンテナを送信する処理を、図 5 5 のフローチャートを用いて説明する。ステップ S 2 5 1 において、コンテンツプロバイダ 2 のウォーターマーク付加部 3 2 は、コンテンツサーバ 3 1 から読み出したコンテンツに、コンテンツプロバイダ 2 を示す所定のウォーターマークを挿入し、圧縮部 3 3 に供給する。ステップ S 2 5 2 において、コンテンツプロバイダ 2 の圧縮部 3 3 は、ウォーターマークが挿入されたコンテンツを ATRAC2 等の所定の方式で圧縮し、暗号化部 3 4 に供給する。ステップ S 2 5 3 において、乱数発生部 3 5 は、コンテンツ鍵 K c o として用いる乱数を発生させ、暗号化部 3 4 に供給する。ステップ S 2 5 4 において、コンテンツプロバイダ 2 の暗号化部 3 4 は、DES などの所定の方式で、コンテンツ鍵 K c o を使用して、ウォーターマークが挿入され、圧縮されたコンテンツを暗号化する。

【0183】

ステップ S 2 5 5 において、暗号化部 3 6 は、DES などの所定の方式で、図 3 9 のステップ S 1 1 の処理により、EMD サービスセンタ 1 から供給されている配送用鍵 K d でコンテンツ鍵 K c o を暗号化する。ステップ S 2 5 6 において、コンテンツプロバイダ 2 のセキュアコンテナ作成部 3 8 は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 K c o、およびポリシー記憶部 3 7 から供給された取扱方針にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵 K s c p で暗号化し、図 1 3 に示すような署名を作成する。ステップ S 2 5 7 において、コンテンツプロバイダ 2 のセキュアコンテナ作成部 3 8 は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 K c o、ポリシー記憶部 3 7 から供給される取扱方針、およびステップ S 2 5 6 で生成した署名を含んだ、図 1 3 に示す

ようなコンテンツプロバイダセキュアコンテナを作成する。

【0184】

ステップS258において、コンテンツプロバイダ2の相互認証部39は、サービスプロバイダ3の相互認証部45と相互認証する。この認証処理は、図42乃至図44を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS259において、コンテンツプロバイダ2のセキュアコンテナ作成部38は、サービスプロバイダ3に、コンテンツプロバイダセキュアコンテナに、予め認証局から発行してもらった証明書を付して送信し、処理を終了する。

【0185】

以上のように、コンテンツプロバイダ2は、サービスプロバイダ3に、コンテンツプロバイダセキュアコンテナを送信する。

【0186】

コンテンツ鍵Kcoと共に取扱方針を配送用鍵Kdで暗号化する例の場合の、コンテンツプロバイダ2がサービスプロバイダ3にコンテンツプロバイダセキュアコンテナを送信する他の処理の詳細を、図56のフローチャートを用いて説明する。ステップS271乃至ステップS274の処理は、図55のステップS251乃至ステップS254の処理とそれぞれ同様であり、その説明は省略する。ステップS275において、コンテンツプロバイダ2の暗号化部36は、図40のステップS21の処理により、EMDサービスセンタ1から供給されている配送用鍵Kdを用いて、DESなどの所定の方式で、コンテンツ鍵Kcoおよびポリシー記憶部37から供給される取扱方針を暗号化する。

【0187】

ステップS276において、コンテンツプロバイダ2のセキュアコンテナ作成部38は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Kco、および暗号化された取扱方針にハッシュ関数を適用しハッシュ値を算出し、自分自身の秘密鍵Kscpで暗号化し、図25に示すような署名を作成する。ステップS277において、コンテンツプロバイダ2のセキュアコンテナ作成部38は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Kco、暗号化された取扱方針、および署名を含んだ、図25に示すようなコンテンツプロバイダセキュアコン

テナを作成する。ステップS278およびステップS279の処理は、図55のステップS258およびステップS259の処理とそれぞれ同様であり、その説明は省略する。

【0188】

このように、コンテンツプロバイダ2は、サービスプロバイダ3に、暗号化された取扱方針を含むコンテンツプロバイダセキュアテナを送信する。

【0189】

次に、図39のステップS15に対応する、サービスプロバイダ3がレシーバ51にサービスプロバイダセキュアテナを送信する処理の詳細を図57のフローチャートを用いて説明する。ステップS291において、サービスプロバイダ3の値付け部42は、コンテンツプロバイダ2のセキュアテナ作成部38から送信されたコンテンツプロバイダセキュアテナに付された証明書に含まれる署名を確認し、証明書の改竄がなければ、コンテンツプロバイダ2の公開鍵K_{pcp}を取り出す。証明書の署名の確認は、図44のステップS83における処理と同様であるので、その説明は省略する。

【0190】

ステップS292において、サービスプロバイダ3の値付け部42は、コンテンツプロバイダ2のセキュアテナ作成部38から送信されたコンテンツプロバイダセキュアテナの署名をコンテンツプロバイダ2の公開鍵K_{pcp}で復号し、得られたハッシュ値が、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K_{co}、および取扱方針にハッシュ関数を適用し得られたハッシュ値と一致することを確認し、コンテンツプロバイダセキュアテナの改竄がないことを確認する。改竄が発見された場合は、処理を終了する。

【0191】

コンテンツプロバイダセキュアテナに改竄がない場合、ステップS293において、サービスプロバイダ3の値付け部42は、コンテンツプロバイダセキュアテナから取扱方針を取り出す。ステップS254において、サービスプロバイダ3の値付け部42は、取扱方針を基に、図17で説明した価格情報を作成する。ステップS295において、サービスプロバイダ3のセキュアテナ

作成部 44 は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 K_{co} 、取扱方針、価格情報、並びに暗号化されたコンテンツ、暗号化されたコンテンツ鍵 K_{co} 、取扱方針、および価格情報にハッシュ関数を適用して得られたハッシュ値を、自分自身の秘密鍵 K_{ssp} で暗号化し、得られた値を署名として図 15 に示すようなサービスプロバイダセキュアコンテナを作成する。

【0192】

ステップ S296 において、サービスプロバイダ 3 の相互認証部 45 は、レシーバ 51 の相互認証モジュール 71 と相互認証する。この認証処理は、図 42 乃至図 44 を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップ S297 において、サービスプロバイダ 3 のセキュアコンテナ作成部 44 は、レシーバ 51 の通信部 61 に、証明書を付したサービスプロバイダセキュアコンテナを送信し、処理を終了する。

【0193】

このように、サービスプロバイダ 3 は、レシーバ 51 にサービスプロバイダセキュアコンテナを送信する。

【0194】

コンテンツプロバイダ 2 において、取扱方針が配送用鍵 K_d で暗号化され、かつ、サービスプロバイダ 3 が取扱制御情報を作成する例の場合の、サービスプロバイダ 3 がレシーバ 51 にサービスプロバイダセキュアコンテナを送信する処理の詳細を、図 58 のフローチャートを用いて説明する。ステップ S311 およびステップ S312 の処理は、図 57 のステップ S291 およびステップ S292 の処理とそれぞれ同様であるので、その説明は省略する。ステップ S313 において、サービスプロバイダ 3 の値付け部 42 は、コンテンツプロバイダセキュアコンテナに含まれる暗号化された取扱方針を復号する。ステップ S314 において、サービスプロバイダ 3 の値付け部 42 は、取扱方針を基に、図 23 で説明した取扱制御情報を作成する。ステップ S315 乃至ステップ S318 の処理は、図 57 のステップ S294 およびステップ S297 の処理とそれぞれ同様であるので、その説明は省略する。

【0195】

このように、サービスプロバイダ3は、レシーバ51に暗号化された取扱方針を含むサービスプロバイダセキュアコンテナを送信する。

【0196】

ユーザネットワーク5が図10または図11の構成を有するときの、図39のステップS16に対応する、適正なサービスプロバイダセキュアコンテナを受信した後の、レシーバ51の課金処理の詳細を、図59のフローチャートを用いて説明する。ステップS331において、レシーバ51の復号／暗号化モジュール74は、配送用鍵Kdでコンテンツ鍵Kcoを復号できるか否かを判定し、配送用鍵Kdでコンテンツ鍵Kcoを復号できないと判定された場合、ステップS332で、レシーバ51は、図53で説明した配送用鍵Kdの受け取り処理を実行し、ステップS333に進む。ステップS331において、配送用鍵Kdでコンテンツ鍵Kcoを復号できると判定された場合、手続は、ステップS332をスキップし、ステップS333に進む。ステップS333において、レシーバ51の復号ユニット91は、図39のステップS13の処理により、記憶モジュール73に記憶されている配送用鍵Kdで、コンテンツ鍵Kcoを復号する。

【0197】

ステップS334において、レシーバ51の課金処理モジュール72は、サービスプロバイダセキュアコンテナに含まれる取扱方針および価格情報を取り出し、図19および図20で説明した課金情報および使用許諾条件情報を生成する。ステップS335において、レシーバ51の課金処理モジュール72は、記憶モジュール73に記憶している課金情報およびステップS334で算出された課金情報から、現在の課金が課金の上限以上であるか否かを判定し、現在の課金が課金の上限以上であると判定された場合、ステップS336に進み、レシーバ51は図53で説明した配送用鍵Kdの受け取り処理を実行し、新たな配送用鍵Kdを受け取り、ステップS337に進む。ステップS335において、現在の課金が課金の上限未満であると判定された場合、ステップS336はスキップされ、ステップS337に進む。

【0198】

ステップS337において、レシーバ51の課金処理モジュール72は、記憶モジュール73に課金情報を記憶させる。ステップS338において、レシーバ51の課金処理モジュール72は、ステップS334にて生成した使用許諾条件情報をHDD52に記録する。ステップS339において、レシーバ51のSAM62は、HDD52にサービスプロバイダセキュアコンテナから取り出した取扱方針を記録させる。

【0199】

ステップS340において、レシーバ51の復号/暗号化モジュール74は、使用許諾条件情報にハッシュ関数を適用しハッシュ値を算出する。ステップS341において、レシーバ51の記憶モジュール73は、使用許諾条件情報のハッシュ値を記憶する。記憶モジュール73に保存用鍵Ksaveが記憶されていない場合、ステップS342において、レシーバ51の乱数発生ユニット92は、保存用鍵Ksaveである乱数を発生し、ステップS343に進む。記憶モジュール73に保存用鍵Ksaveが記憶されている場合、ステップS342はスキップされ、ステップS343に進む。

【0200】

ステップS343において、レシーバ51の暗号化ユニット93は、コンテンツ鍵Kcoを保存用鍵Ksaveで暗号化する。ステップS344において、レシーバ51のSAM62は、暗号化されたコンテンツ鍵KcoをHDD52に記憶させる。記憶モジュール73に保存用鍵Ksaveが記憶されていない場合、ステップS345において、レシーバ51の復号/暗号化モジュール74は、保存用鍵Ksaveを記憶モジュール73に記憶させ、処理は終了する。記憶モジュール73に保存用鍵Ksaveが記憶されている場合、ステップS345はスキップされ、処理は終了する。

【0201】

以上のように、レシーバ51は、課金情報を記憶モジュール73に記憶すると共に、コンテンツ鍵Kcoを配送用鍵Kdで復号し、再度、コンテンツ鍵Kcoを保存用鍵Ksaveで暗号化し、HDD52に記録させる。保存用鍵Ksave

は、記憶モジュール73に記憶される。

【0202】

レコーダ53も、同様の処理で、課金情報をSAM66内の記憶モジュールに記憶すると共に、コンテンツ鍵Kcoを配送用鍵Kdで復号し、再度、コンテンツ鍵Kcoを保存用鍵Ksaveで暗号化し、HDD52に記録させる。保存用鍵Ksaveは、SAM66内の記憶モジュールに記憶される。

【0203】

ユーザネットワーク5が図30の構成を有し、記憶モジュール73に検査値を記憶する場合の、図39のステップS15およびステップS16に対応する、レシーバ51の、適正なサービスプロバイダセキュアコンテナを受信し、課金する処理の詳細を、図60のフローチャートを用いて説明する。ステップS361において、レシーバ51の相互認証モジュール71は、通信部61を介して、サービスプロバイダ3の相互認証部44と相互認証し、相互認証できたとき、通信部61は、相互認証したサービスプロバイダ3から、サービスプロバイダセキュアコンテナを受信する。相互認証できなかった場合、処理は終了する。ステップS362において、通信部61は、ステップS361で相互認証したサービスプロバイダ3から、公開鍵証明書を受信する。

【0204】

ステップS363において、復号/暗号化モジュール62は、ステップS361で受信したサービスプロバイダセキュアコンテナに含まれる署名データを検証し、改竄がなかったか否かを検証する。ここで、改竄が発見された場合、処理は終了する。ステップS364において、レシーバ51は、図示せぬ表示部に受信したサービスプロバイダセキュアコンテナに含まれる取扱情報および価格情報を表示し、ユーザは、コンテンツの再生またはコピーなど、購入の内容を決定し、レシーバ51にその内容を指示する。ステップS365において、レシーバ51の課金処理モジュール72は、取扱情報および価格情報、並びに購入の内容を基に、課金情報および使用許諾条件情報を生成する。

【0205】

ステップS366において、SAM62は、サービスプロバイダセキュアコンテ

ナに含まれるコンテンツ鍵K c oで暗号化されているコンテンツをHDD5 2に記録させる。ステップS 3 6 7において、復号/暗号化ユニット7 4の復号ユニット9 1は、サービスプロバイダセキュアコンテナに含まれる配送用鍵K dで暗号化されているコンテンツ鍵K c oを、図4 5のステップS 1 1 0または図5 3のステップS 2 1 0で記憶モジュール7 3に記憶している配送用鍵K dで復号する。ステップS 3 6 8において、暗号化ユニット9 3は、ステップS 3 6 7で復号されたコンテンツ鍵を記憶モジュール7 3に記憶している保存用鍵K s a v eで暗号化する。

【0 2 0 6】

ステップS 3 6 9において、データ検査モジュール1 1 4は、外部記憶部1 1 3の、空きを有する鍵データブロックを検索する。ステップS 3 7 0において、データ検査モジュール1 1 4は、ステップS 3 6 9で検索した鍵データブロックに記憶されているデータ（コンテンツ鍵K c o、コンテンツIDなどのデータ）にハッシュ関数を適用し、ハッシュ値を得る。ステップS 3 7 1において、データ検査モジュール1 1 4は、ステップS 3 7 0で得られたハッシュ値と、記憶モジュール7 3に記憶されている、ステップS 3 6 9で検索された鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップS 3 7 2に進み、SAM 6 2は、ステップS 3 6 8にて暗号化されたコンテンツ鍵K c oを、外部記憶部1 1 3の空きを有する鍵データブロックに記憶させる。

【0 2 0 7】

ステップS 3 7 3において、復号/暗号化モジュール7 4は、外部記憶部1 1 3の、コンテンツ鍵K c oを記憶させた鍵データブロックに記憶しているデータにハッシュ関数を適用し、ハッシュ値を得る。ステップS 3 7 4において、復号/暗号化モジュール7 4は、ステップS 3 7 3にて算出したハッシュ値を、記憶モジュール7 3の、コンテンツ鍵K c oを記憶させた鍵データブロックに対応する検査値に上書きする。ステップS 3 7 5において、課金モジュール7 2は、ステップS 3 6 5で作成した課金情報を記憶モジュール7 3に記憶させ、処理は終了する。

【0208】

ステップS371において、ステップS370で得られたハッシュ値と、記憶モジュール73に記憶されている、ステップS369で検索された鍵データブロックに対応する検査値とを比較し、一致しないと判定された場合、その鍵データブロックのデータは改竄されているので、手続きは、ステップS376に進み、データ検査モジュール114は、外部記憶部113の全ての鍵データブロックを調べたか否かを判定し、外部記憶部113の全ての鍵データブロックを調べていないと判定された場合、ステップS377に進み、データ検査モジュール114は、外部記憶部113の、他の空きを有する鍵データブロックを検索し、ステップS370に戻り、処理を繰り返す。

【0209】

ステップS376において、外部記憶部113の全ての鍵データブロックを調べたと判定された場合、コンテンツ鍵Kcoを記憶できる鍵データブロックは無いので、処理は終了する。

【0210】

このように、図30のレシーバ51は、外部記憶部113のコンテンツ鍵Kco等が記憶されている鍵データブロックの改竄を検査し、改竄のない鍵データブロックのみに、新たなコンテンツ鍵Kcoを記憶する。

【0211】

ユーザネットワーク5が図30の構成を有し、外部記憶部113に検査値を記憶する場合の、図39のステップS15およびステップS16に対応する、レシーバ51の、適正なサービスプロバイダセキュアコンテナを受信し、課金する処理の詳細を、図61のフローチャートを用いて説明する。ステップS391乃至ステップS400の処理は、図60のステップS361乃至ステップS370の処理とそれぞれ同様であり、その説明は省略する。

【0212】

ステップS401において、復号ユニット91は、外部記憶部113に記憶されている、ステップS399で検索した鍵データブロックに対応する検査値を、記憶モジュール73に記憶する検査用鍵Kchで復号する。ステップS402に

において、データ検査モジュール 114 は、ステップ S400 で得られたハッシュ値と、ステップ S401 で復号された検査値とを比較し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、手続きは、ステップ S403 に進む。

【0213】

ステップ S403 およびステップ S404 の処理は、図 60 のステップ S372 およびステップ S373 の処理とそれぞれ同様であり、その説明は省略する。

【0214】

ステップ S405 において、暗号化ユニット 93 は、ステップ S404 において得られたハッシュ値を、記憶モジュール 73 に記憶する検査用鍵 K_{ch} で暗号化する。ステップ S406 において、復号／暗号化モジュール 74 は、ステップ S405 にて暗号化したハッシュ値を、記憶モジュール 73 の、コンテンツ鍵 K_{co} を記憶させた鍵データブロックに対応する検査値に上書きする。

【0215】

ステップ S407 乃至ステップ S409 の処理は、図 60 のステップ S375 乃至ステップ S377 の処理とそれぞれ同様であり、その説明は省略する。

【0216】

このように、図 61 に示す処理においても、図 30 のレシーバ 51 は、外部記憶部 113 のコンテンツ鍵 K_{co} 等が記憶されている鍵データブロックの改竄を検査し、改竄のない鍵データブロックのみに、新たなコンテンツ鍵 K_{co} を記憶する。

【0217】

次に、ユーザネットワーク 5 が図 30 の構成を有する場合の、MDドライブ 54 から供給される暗号化されていないコンテンツを、暗号化し、記録する処理の詳細を、図 62 のフローチャートを用いて説明する。ステップ S421 において、SAM 62 の乱数発生ユニット 92 は、乱数を生成し、コンテンツ鍵 K_{co} とする。ステップ S422 において、通信部 61 は、MDドライブ 54 から、MDドライブ 54 に装着されている MD が記録するコンテンツを受信する。ステップ S423 において、SAM 62 の暗号化ユニット 93 は、ステップ S422 で受信したコンテ

ンツを、ステップS421で生成したコンテンツ鍵Kc oで暗号化する。ステップS424において、SAM62は、暗号化されたコンテンツをHDD52に記録させる。ステップS425において、SAM62の暗号化ユニット93は、コンテンツ鍵Kc oを記憶モジュール73に記憶している保存用鍵K s a v eで暗号化する。

【0218】

ステップS426乃至ステップS434の処理は、図60のステップS369乃至ステップS377の処理とそれぞれ同等であり、その説明は、省略する。

【0219】

このように、レシーバ51は、MDドライブ54から供給される暗号化されていないコンテンツを、暗号化し、HDD52に記録する。

【0220】

図39のステップS17に対応するレシーバ51がコンテンツを再生する処理の詳細を、図63のフローチャートを用いて説明する。ステップS451において、レシーバ51の復号/暗号化モジュール74は、HDD52から、図59のステップS338で記憶した使用許諾条件情報およびステップS344で記憶した暗号化されたコンテンツ鍵Kc oを読み出す。ステップS452において、レシーバ51の復号/暗号化モジュール74は、使用許諾条件情報にハッシュ関数を適用しハッシュ値を算出する。

【0221】

ステップS453において、レシーバ51の復号/暗号化モジュール74は、ステップS452において算出されたハッシュ値が、図59のステップS340で記憶モジュール73に記憶されたハッシュ値と一致するか否かを判定し、ステップS452において算出されたハッシュ値が、記憶モジュール73に記憶されたハッシュ値と一致すると判定された場合、ステップS454に進み、使用回数の値などの使用許諾条件情報に含まれる所定の情報を更新する。ステップS455において、レシーバ51の復号/暗号化モジュール74は、更新した使用許諾条件情報にハッシュ関数を適用しハッシュ値を算出する。ステップS456において、レシーバ51の記憶モジュール73は、ステップS455で算出した使用

許諾条件情報のハッシュ値を記憶する。ステップS457において、レシーバ51の復号／暗号化モジュール74は、HDD52に更新した使用許諾条件情報を記録させる。

【0222】

ステップS458において、SAM62の相互認証モジュール71と伸張部63の相互認証モジュール75は、相互認証し、SAM62および伸張部63は、一時鍵Ktempを記憶する。この認証処理は、図42乃至図44を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数R1、R2、またはR3が、一時鍵Ktempとして用いられる。ステップS459において、復号／暗号化モジュール74の復号ユニット91は、図59のステップS344にてHDD52に記録されたコンテンツ鍵Kcoを、記憶モジュール73に記憶された保存用鍵Ksaveで復号する。ステップS460において、復号／暗号化モジュール74の暗号化ユニット93は、復号されたコンテンツ鍵Kcoを一時鍵Ktempで暗号化する。ステップS461において、SAM62は、一時鍵Ktempで暗号化されたコンテンツ鍵Kcoを伸張部63に送信する。

【0223】

ステップS462において、伸張部63の復号モジュール76は、コンテンツ鍵Kcoを一時鍵Ktempで復号する。ステップS463において、SAM62は、HDD52に記録されたコンテンツを読み出し、伸張部63に送信する。ステップS464において、伸張部63の復号モジュール77は、コンテンツをコンテンツ鍵Kcoで復号する。ステップS465において、伸張部63の伸張モジュール78は、復号されたコンテンツをATRAC2などの所定の方式で伸張する。ステップS466において、伸張部63のウォーターマーク付加モジュール79は、伸張されたコンテンツにレシーバ51を特定する所定のウォーターマークを挿入する。ステップS467において、レシーバ51は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

【0224】

ステップS453において、ステップS452において算出されたハッシュ値

が、記憶モジュール 73 に記憶されたハッシュ値と一致しないと判定された場合、ステップ S468 において、SAM62 は、図示せぬ表示装置にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

【0225】

このように、レシーバ 51 は、コンテンツを再生する。

【0226】

図 64 は、図 11 の構成を有するユーザホームネットワーク 5 において、レシーバ 51 がデコーダ 56 にコンテンツを再生させる処理を説明するフローチャートである。ステップ S481 乃至ステップ S487 の処理は、図 63 のステップ S451 乃至ステップ S457 の処理とそれぞれ同様であるので、その説明は省略する。

【0227】

ステップ S488 において、SAM62 の相互認証モジュール 71 とデコーダ 56 の相互認証モジュール 101 は、相互認証し、一時鍵 K_{temp} が共有される。この認証処理は、図 42 乃至図 44 を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数 R_1 、 R_2 、または R_3 が、一時鍵 K_{temp} として用いられる。ステップ S489 において、復号/暗号化モジュール 74 の復号ユニット 91 は、HDD 52 に記録されたコンテンツ鍵 K_c を、記憶モジュール 73 に記憶された保存用鍵 K_{save} で復号する。ステップ S490 において、復号/暗号化モジュール 74 の暗号化ユニット 93 は、復号されたコンテンツ鍵 K_c を一時鍵 K_{temp} で暗号化する。ステップ S491 において、SAM62 は、一時鍵 K_{temp} で暗号化されたコンテンツ鍵 K_c をデコーダ 56 に送信する。

【0228】

ステップ S492 において、デコーダ 56 の復号モジュール 102 は、コンテンツ鍵 K_c を一時鍵 K_{temp} で復号する。ステップ S493 において、SAM62 は、HDD 52 に記録されたコンテンツを読み出し、デコーダ 56 に送信する。ステップ S494 において、デコーダ 56 の復号モジュール 103 は、コンテンツをコンテンツ鍵 K_c で復号する。ステップ S495 において、デコーダ 5

6の伸張モジュール104は、復号されたコンテンツをATRAC2などの所定の方法で伸張する。ステップS496において、デコーダ56のウォータマーク付加モジュール105は、伸張されたコンテンツにデコーダ56を特定する所定のウォータマークを挿入する。ステップS497において、デコーダ56は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

【0229】

ステップS498の処理は、図63のステップS468の処理と同様であるので、その説明は省略する。

【0230】

以上のように、ユーザホームネットワークが図11に示す構成を有する場合、レシーバ51が受信したコンテンツは、デコーダ56で再生される。

【0231】

続いて、ユーザネットワーク5が図30の構成を有し、検査値が記憶モジュール73および記憶部135に記憶されているときの、HDD52に記録されているコンテンツを、レシーバ51に装着されているメモリスティック111に移動する処理を、図65および図66のフローチャートを参照して説明する。ステップS511において、レシーバ51の相互認証モジュール71は、レシーバ51に装着されているメモリスティック111の相互認証部133と相互認証し、一時鍵Ktempを共有する。この認証処理は、図42乃至図44を参照して説明した場合と同様であるので、ここでは説明を省略する。

【0232】

ステップS512において、レシーバ51は、HDD52からコンテンツに関するデータを検索し、図示せぬ表示部に表示し、ユーザは、メモリスティック111に移動するコンテンツを選択し、レシーバ51に所定のデータを図示せぬスイッチで、入力する。ステップS513において、レシーバ51のSAM62は、選択されたコンテンツに対応するコンテンツ鍵を、外部記憶部113から検索する。ステップS514において、レシーバ51のデータ検査モジュール114は、移動するコンテンツに対応するコンテンツ鍵Kcoを記憶する、外部記憶部113の鍵データブロックに記憶しているデータ（コンテンツ鍵Kco、コンテンツ

IDなどのデータ)に、ハッシュ関数を適用し、ハッシュ値を得る。ステップS515において、データ検査モジュール114は、ステップS514で得られたハッシュ値と、記憶モジュール73に記憶されている、コンテンツ鍵Kcoを記憶している鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップS516に進み、レシーバ51の通信部61は、メモリスティック111の通信部131に書き込み要求コマンドおよびコンテンツIDを送信し、メモリスティック111の通信部131は、書き込み要求コマンドおよびコンテンツIDを受信する。

【0233】

ステップS517において、レシーバ51の通信部61は、メモリスティック111の通信部131にステップS512で選択されたコンテンツを送信し、メモリスティック111の通信部131は、コンテンツを受信する。ステップS518において、メモリスティック111のメモリコントローラ132は、通信部131が受信したコンテンツを、情報記憶ブロック122に、暗号化データ144として記憶させる。

【0234】

ステップS519において、レシーバ51の復号ユニット91は、コンテンツ鍵Kcoを記憶モジュール73に記憶している保存用鍵Ksaveで復号し、暗号化ユニット93は、復号したコンテンツ鍵Kcoを、一時鍵Ktempで再度、暗号化し、SAM62内の図示せぬレジスタに一時的に記憶する。ステップS520において、SAM62は、移動するコンテンツに対応する、外部記憶部113に記憶されているコンテンツ鍵Kcoを削除する。ステップS521において、レシーバ51の復号/暗号化モジュール74は、移動するコンテンツに対応するコンテンツ鍵Kcoを削除した、外部記憶部113の鍵データブロックに記憶しているデータに、ハッシュ関数を適用し、ハッシュ値を得る。ステップS522において、復号/暗号化モジュール74は、ステップS521にて算出したハッシュ値を、記憶モジュール73の、コンテンツ鍵Kcoを削除した鍵データブロックに対応する検査値に上書きする。

【0235】

ステップS523において、レシーバ51の通信部61は、コンテンツ鍵Kco、コンテンツID、および使用許諾条件情報を、メモリスティック111の通信部131に送信し、メモリスティック111の通信部131は、コンテンツ鍵Kco、コンテンツID、および使用許諾条件情報を受信する。ステップS524において、メモリスティック111の復号部136は、受信部131が受信したコンテンツ鍵Kcoを一時鍵Ktempで復号し、暗号化部134は、復号したコンテンツ鍵Kcoを記憶部135が記憶する保存用鍵Ksaveで暗号化し、制御ブロック121内の図示せぬレジスタに一時的に記憶させる。

【0236】

ステップS525において、データ検査部138は、鍵データ143の、空きを有する鍵データブロックを検索する。ステップS526において、データ検査部138は、ステップS525で検索した鍵データブロックに記憶されているデータ（コンテンツ鍵Kco、コンテンツIDなどのデータ）にハッシュ関数を適用し、ハッシュ値を得る。ステップS527において、データ検査部138は、ステップS526で算出したハッシュ値と、記憶部135に記憶されている、ステップS525で検索された鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致していると判定された場合、ステップS528に進み、メモリコントローラ132は、レジスタに一時的に記憶されているコンテンツ鍵Kcoを、鍵データ143の空きのある鍵データブロックに記憶させる。

【0237】

ステップS529において、データ検査部138は、鍵データ143の、コンテンツ鍵Kcoを記憶させた鍵データブロックに記憶しているデータにハッシュ関数を適用し、ハッシュ値を得る。ステップS530において、データ検査部138は、ステップS529にて算出したハッシュ値を、記憶部135の、コンテンツ鍵Kcoを記憶させた鍵データブロックに対応する検査値に上書きする。

【0238】

ステップS531において、メモリスティック111の通信部131は、レシーバ51の通信部61に、受信完了信号を送信し、レシーバ51の通信部61は

、受信完了信号を受信する。ステップS532において、レシーバ51のSAM62は、HDD62からコンテンツを削除させ、コンテンツ鍵Kcoをレジスタから削除し、処理は終了する。

【0239】

ステップS527において、ステップS526で得られたハッシュ値と、記憶部135に記憶されている、ステップS523で検索された鍵データブロックに対応する検査値とを比較し、一致しないと判定された場合、その鍵データブロックのデータは改竄されているので、手続きは、ステップS533に進み、データ検査部135は、鍵データ143の全ての鍵データブロックを調べたか否かを判定し、鍵データ143の全ての鍵データブロックを調べていないと判定された場合、ステップS534に進み、データ検査部135は、鍵データ143の、他の空きを有する鍵データブロックを検索し、ステップS526に戻り、処理を繰り返す。

【0240】

ステップS533において、鍵データ143の全ての鍵データブロックを調べたと判定された場合、コンテンツ鍵Kcoを記憶できる鍵データブロックは無いので、処理は終了する。

【0241】

ステップS515において、データ検査モジュール114は、ステップS514で得られたハッシュ値と、記憶モジュール73に記憶されている、コンテンツ鍵Kcoを記憶している鍵データブロックに対応する検査値が一致しないと判定された場合、移動しようとしているコンテンツは改竄されているので、処理は終了する。

【0242】

以上のように、HDD62に記憶されているコンテンツは、メモリスティック111に移動される。

【0243】

ユーザネットワーク5が図30の構成を有し、検査値が外部記憶部113および鍵データ143に記憶されているときの、HDD52に記録されているコンテン

ツを、レシーバ51に装着されているメモリスティック111に移動する処理を、図67および図68のフローチャートを参照して説明する。ステップS551乃至ステップS554の処理は、図65のステップS511乃至ステップS514の処理とそれぞれ同様なので、その説明は省略する。

【0244】

ステップS555において、データ検査モジュール114は、コンテンツ鍵Kcoを記憶している鍵データブロックに対応する検査値を記憶モジュール73が記憶する検査用鍵Kchで復号する。ステップS556において、データ検査モジュール114は、ステップS554で得られたハッシュ値と、ステップS555で復号された検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップS557に進む。

【0245】

ステップS557乃至ステップS562の処理は、図65のステップS516乃至ステップS521の処理とそれぞれ同様なので、その説明は省略する。

【0246】

ステップS563において、暗号化ユニット93は、ステップS562で算出されたハッシュ値を、記憶モジュール73に記憶する検査用鍵Kchで暗号化する。ステップS564において、復号／暗号化モジュール74は、ステップS563にて暗号化したハッシュ値を、外部記憶部113の、コンテンツ鍵Kcoを削除した鍵データブロックに対応する検査値に上書きする。

【0247】

ステップS565乃至ステップS568の処理は、図65または図66のステップS523乃至ステップS526の処理とそれぞれ同様なので、その説明は省略する。

【0248】

ステップS569において、復号部136は、ステップS567で検索した鍵データブロックに対応する検査値を記憶部135が記憶する検査用鍵Kchで復号する。ステップS570において、データ検査部138は、ステップS568

で得られたハッシュ値と、ステップS569で復号された検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップS571に進む。

【0249】

ステップS571およびステップS572の処理は、図66のステップS528およびステップS529の処理と、それぞれ同様なので、その説明は省略する。

【0250】

ステップS573において、データ検査部138は、ステップS572で算出されたハッシュ値を、記憶部135に記憶している検査用鍵Kchで暗号化する。ステップS574において、データ検査部138は、ステップS573にて暗号化したハッシュ値を、鍵データ143の、コンテンツ鍵Kcoを記憶させた鍵データブロックに対応する検査値に上書きする。

【0251】

ステップS575乃至ステップS578の処理は、図66のステップS531乃至ステップS534の処理と、それぞれ同様なので、その説明は省略する。

【0252】

ステップS556において、データ検査モジュール114は、ステップS554で得られたハッシュ値と、ステップS555で復号した検査値が一致しないと判定された場合、移動しようとしているコンテンツは改竄されているので、処理は終了する。

【0253】

このように、HDD62に記憶されているコンテンツは、メモリスティック111に移動される。

【0254】

次に、ユーザネットワーク5が図30の構成を有し、検査値が記憶モジュール73および記憶部135に記憶されているときの、レシーバ51に装着されているメモリスティック111に記憶されているコンテンツを、HDD52に移動する処理を、図69および図70のフローチャートを参照して説明する。ステップS

591において、レシーバ51の相互認証モジュール71は、レシーバ51に装着されているメモリスティック111の相互認証部133と相互認証し、一時鍵 *Ktemp* を共有する。この認証処理は、図42乃至図44を参照して説明した場合と同様であるので、ここでは説明を省略する。

【0255】

ステップS592において、レシーバ51は、通信部61を介して、メモリスティック111のデータ検索性テーブルからコンテンツに関するデータを検索し、図示せぬ表示部に表示し、ユーザは、HDD52に移動するコンテンツを選択し、レシーバ51に所定のデータを図示せぬスイッチで、入力する。ステップS593において、レシーバ51の通信部61は、メモリスティック111の通信部131に移動要求コマンドおよびコンテンツIDを送信し、メモリスティック111の通信部131は、移動要求コマンドおよびコンテンツIDを受信する。

【0256】

ステップS594において、メモリスティック111のメモリコントローラ132は、受信したコンテンツIDに対応したコンテンツ鍵 *Kco* を、鍵データ143から検索する。ステップS595において、データ検査部138は、コンテンツIDに対応したコンテンツ鍵 *Kco* を記憶している鍵データブロックに記憶されているデータ（コンテンツ鍵 *Kco*、コンテンツIDなどのデータ）にハッシュ関数を適用し、ハッシュ値を得る。ステップS596において、データ検査部138は、ステップS595で算出したハッシュ値と、記憶部135に記憶されている、コンテンツIDに対応したコンテンツ鍵 *Kco* を記憶している鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致していると判定された場合、コンテンツ鍵 *Kco* などに改竄はないので、ステップS597に進み、メモリコントローラ132は、データ検索性テーブル141を参照して、コンテンツIDに対応したコンテンツを暗号化データ144から検索する。

【0257】

ステップS598において、メモリスティック111の通信部131は、レシーバ51の通信部61にステップS597で検索されたコンテンツを送信し、レシーバ51の通信部61は、コンテンツを受信する。ステップS599において

、SAM 6 2は、受信部 6 1が受信したコンテンツをHDD 5 2に記憶させる。

【0258】

ステップS 6 0 0において、メモリスティック1 1 1の復号部1 3 6は、コンテンツ鍵K c oを記憶部1 3 5に記憶している保存用鍵K s a v eで復号し、暗号化部1 3 4は、復号したコンテンツ鍵K c oを、一時鍵K t e m pで再度、暗号化し、制御ブロック1 2 1内の図示せぬレジスタに一時的に記憶する。ステップS 6 0 1において、メモリコントローラ1 3 2は、移動するコンテンツに対応する、鍵データ1 4 3に記憶されているコンテンツ鍵K c oを削除する。ステップS 6 0 2において、制御ブロック1 2 1のデータ検査部1 3 8は、移動するコンテンツに対応するコンテンツ鍵K c oを削除した、鍵データ1 4 3の鍵データブロックに記憶しているデータに、ハッシュ関数を適用し、ハッシュ値を得る。ステップS 6 0 3において、データ検査部1 3 8は、ステップS 6 0 2にて算出したハッシュ値を、鍵データ1 4 3の、コンテンツ鍵K c oを削除した鍵データブロックに対応する検査値に上書きする。

【0259】

ステップS 6 0 4において、メモリスティック1 1 1の通信部1 3 1は、コンテンツ鍵K c o、コンテンツID、および使用許諾条件情報を、レシーバ5 1の通信部6 1に送信し、レシーバ5 1の通信部6 1は、コンテンツ鍵K c o、コンテンツID、および使用許諾条件情報を受信する。ステップS 6 0 5において、レシーバ5 1のデータ検査モジュール7 3は、外部記憶部1 1 3の、空きを有する鍵データブロックを検索する。ステップS 6 0 6において、データ検査モジュール1 1 4は、ステップS 6 0 5で検索した鍵データブロックに記憶されているデータにハッシュ関数を適用し、ハッシュ値を得る。ステップS 6 0 7において、データ検査モジュール1 1 4は、ステップS 6 0 6で得られたハッシュ値と、記憶モジュール7 3に記憶されている、ステップS 6 0 5で検索された鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップS 6 0 8に進み、レシーバ5 1の復号ユニット9 1は、受信部6 1が受信したコンテンツ鍵K c oを一時鍵K t e m pで復号し、暗号化ユニット9 3は、復号した

コンテンツ鍵K c oを記憶モジュール73が記憶する保存用鍵K s a v eで暗号化する。ステップS609に進み、SAM62は、ステップS607にて暗号化されたコンテンツ鍵K c oを、外部記憶部113の空きを有する鍵データブロックに記憶させる。

【0260】

ステップS610において、復号/暗号化モジュール74は、外部記憶部113の、コンテンツ鍵K c oを記憶させた鍵データブロックに記憶しているデータにハッシュ関数を適用し、ハッシュ値を得る。ステップS611において、復号/暗号化モジュール74は、ステップS610にて算出したハッシュ値を、記憶モジュール73の、コンテンツ鍵K c oを記憶させた鍵データブロックに対応する検査値に上書きする。ステップS612において、レシーバ51の通信部61は、メモリスティック111の通信部131に受信完了信号を送信し、メモリスティック111の通信部131は、受信完了信号を受信する。ステップS613において、メモリスティック111のメモリコントローラ132は、暗号化データ144から、送信したコンテンツを削除し、鍵データ143から、対応するコンテンツ鍵K c oを削除し、処理は終了する。

【0261】

ステップS607において、ステップS606で得られたハッシュ値と、記憶モジュール73に記憶されている、ステップS605で検索された鍵データブロックに対応する検査値とを比較し、一致しないと判定された場合、その鍵データブロックのデータは改竄されているので、手続きは、ステップS614に進み、データ検査モジュール114は、外部記憶部113の全ての鍵データブロックを調べたか否かを判定し、外部記憶部113の全ての鍵データブロックを調べていないと判定された場合、ステップS615に進み、データ検査モジュール114は、外部記憶部113の、他の空きを有する鍵データブロックを検索し、ステップS606に戻り、処理を繰り返す。

【0262】

ステップS614において、外部記憶部113の全ての鍵データブロックを調べたと判定された場合、コンテンツ鍵K c oを記憶できる鍵データブロックは無

いので、処理は終了する。

【0263】

ステップS596において、ステップS595で算出したハッシュ値と、記憶部135に記憶されている、コンテンツIDに対応したコンテンツ鍵Kcoを記憶している鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致していないと判定された場合、送信したいコンテンツのコンテンツ鍵Kcoなどに改竄があるので、処理は終了する。

【0264】

このように、コンテンツは、メモリスティック111から、レシーバ51に移動される。

【0265】

ユーザネットワーク5が図30の構成を有し、検査値が外部記憶部113および鍵データ143に記憶されているときの、レシーバ51に装着されているメモリスティック111に記憶されているコンテンツを、HDD52に移動する処理を、図71および図72のフローチャートを参照して説明する。ステップS631乃至ステップS635の処理は、図69のステップS591乃至ステップS595の処理とそれぞれ同様なので、その説明は省略する。

【0266】

ステップS636において、復号部136は、コンテンツ鍵Kcoを記憶している鍵データブロックに対応する検査値を記憶部135が記憶する検査用鍵Kchで復号する。ステップS637において、データ検査部138は、ステップS635で得られたハッシュ値と、ステップS636で復号された検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップS638に進む。

【0267】

ステップS638乃至ステップS643の処理は、図69のステップS597乃至ステップS602の処理とそれぞれ同様なので、その説明は省略する。

【0268】

ステップS644において、データ検査部138は、ステップS643で算出

されたハッシュ値を、記憶部135に記憶する検査用鍵Kchで暗号化する。ステップS645において、データ検査部138は、ステップS644にて暗号化したハッシュ値を、鍵データ143の、コンテンツ鍵Kcoを削除した鍵データブロックに対応する検査値に上書きする。

【0269】

ステップS646およびステップS647の処理は、図70のステップS604およびステップS605の処理とそれぞれ同様なので、その説明は省略する。

【0270】

ステップS649において、データ検査モジュール114は、ステップS647で検索した鍵データブロックに対応する検査値を記憶部135が記憶する検査用鍵Kchで復号する。ステップS650において、データ検査モジュール114は、ステップS648で得られたハッシュ値と、ステップS649で復号された検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップS651に進む。

【0271】

ステップS651乃至ステップS653の処理は、図70のステップS608乃至ステップS610の処理とそれぞれ同様なので、その説明は省略する。

【0272】

ステップS654において、暗号化ユニット93は、ステップS655で算出されたハッシュ値を、記憶モジュール73に記憶している検査用鍵Kchで暗号化する。ステップS655において、復号／暗号化モジュール74は、ステップS654にて暗号化したハッシュ値を、外部記憶部113の、コンテンツ鍵Kcoを記憶させた鍵データブロックに対応する検査値に上書きする。

【0273】

ステップS656乃至ステップS659の処理は、図70のステップS612乃至ステップS615の処理と、それぞれ同様なので、その説明は省略する。

【0274】

以上のように、検査値が外部記憶部113および鍵データ143に記憶されて

いるときでも、コンテンツは、メモリスティック111から、レシーバ51に移動される。

【0275】

次に、ユーザネットワーク5が図30の構成を有し、検査値が記憶部135に記憶されているときの、レシーバ51に装着されているメモリスティック111に記憶されているコンテンツを、レシーバ51が再生する処理を、図73のフローチャートを参照して説明する。ステップS671において、SAM62の相互認証モジュール71は、レシーバ51に装着されているメモリスティック111の相互認証部133と相互認証し、一時鍵Ktempを共有する。この認証処理は、図42乃至図44を参照して説明した場合と同様であるので、ここでは説明を省略する。コンテンツの再生におけるステップS671の相互認証で使用される鍵は、図69に示すコンテンツの移動におけるステップS591の相互認証で使用する鍵と、異なる鍵を使用してもよい。

【0276】

ステップS672において、レシーバ51のSAM62は、通信部61を介して、メモリスティック111のデータ検索用テーブルからコンテンツに関するデータを検索し、図示せぬ表示部に表示させ、ユーザは、再生するコンテンツを選択し、レシーバ51に所定のデータを図示せぬスイッチで、入力する。ステップS673において、レシーバ51のSAM62は、通信部61を介して、メモリスティック111の通信部131に読み出し要求コマンドおよびコンテンツIDを送信し、メモリスティック111の通信部131は、読み出し要求コマンドおよびコンテンツIDを受信する。

【0277】

ステップS674において、メモリスティック111のメモリコントローラ132は、受信したコンテンツIDに対応したコンテンツ鍵Kcoを、鍵データ143から検索する。ステップS675において、データ検査部138は、コンテンツIDに対応したコンテンツ鍵Kcoを記憶している鍵データブロックに記憶されているデータ（コンテンツ鍵Kco、コンテンツIDなどのデータ）にハッシュ関数を適用し、ハッシュ値を得る。ステップS676において、データ検査部13

8は、ステップS675で算出したハッシュ値と、記憶部135に記憶されている、コンテンツIDに対応したコンテンツ鍵Kcoを記憶している鍵データブロックに対応する検査値とを比較し、一致するか否かを判定し、一致していると判定された場合、コンテンツ鍵Kcoなどに改竄はないので、ステップS677に進み、メモリコントローラ132は、データ検索用テーブル141を参照して、コンテンツIDに対応したコンテンツを暗号化データ144から検索する。

【0278】

ステップS678において、メモリスティック111の通信部131は、レシーバ51の通信部61にステップS677で検索されたコンテンツを送信し、レシーバ51の通信部61は、コンテンツを受信する。ステップS679において、メモリスティック111の復号部136は、コンテンツ鍵Kcoを記憶部135に記憶している保存用鍵Ksaveで復号し、暗号化部134は、復号したコンテンツ鍵Kcoを、一時鍵Ktempで再度、暗号化し、制御ブロック121内の図示せぬレジスタに一時的に記憶する。ステップS680において、メモリスティック111の通信部131は、コンテンツ鍵Kco、コンテンツID、および使用許諾条件情報を、レシーバ51のSAM62に送信し、レシーバ51のSAM62は、コンテンツ鍵Kco、コンテンツID、および使用許諾条件情報を受信する。

【0279】

ステップS681において、SAM62の相互認証モジュール71は、伸張部63の相互認証モジュール75と相互認証し、一時鍵Ktemp（ステップS671で共有する一時鍵Ktempとは異なる）を共有する。この認証処理は、図42乃至図44を参照して説明した場合と同様であるので、ここでは説明を省略する。

【0280】

ステップS682において、SAM62の復号ユニット91は、コンテンツ鍵Kcoを、メモリスティック111と共有している一時鍵Ktempで復号し、暗号化ユニット93は、復号されたコンテンツ鍵Kcoを、伸張部63と共有している一時鍵Ktempで再度、暗号化する。ステップS683において、SAM6

2は、伸張部63と共有している一時鍵K t e m pで暗号化されたコンテンツ鍵K c oを、伸張部63に送信し、伸張部63は、暗号化されたコンテンツ鍵K c oを、受信する。

【0281】

ステップS684において、伸張部63の復号モジュール77は、受信部61が受信したコンテンツ鍵K c oを、SAM62と共有する一時鍵K t e m pで復号する。ステップS685において、伸張部63の復号モジュール76は、ステップS678で受信したコンテンツを、ステップS684で復号したコンテンツ鍵K c oで復号する。ステップS686において、伸張部63の伸張モジュール78は、復号されたコンテンツをATRAC2などの所定の方式で伸張する。ステップS687において、ウォータマーク付加モジュール79は、伸張されたコンテンツにレシーバ51を特定する所定のウォータマークを挿入する。ステップS688において、伸張部63は、図示せぬスピーカなどに再生されたコンテンツを出力する。ステップS689において、レシーバ51のSAM62は、メモリスティック111の通信部131に再生完了信号を送信し、メモリスティック111の制御ブロック121は、再生完了信号を受信し、処理は終了する。

【0282】

ステップS676において、ステップS675で算出したハッシュ値と、記憶部135に記憶されている、コンテンツIDに対応したコンテンツ鍵K c oを記憶している鍵データブロックに対応する検査値とを比較し、一致しないと判定された場合、コンテンツ鍵K c oなどに改竄があるので、処理は終了する。

【0283】

このように、鍵データブロックの改竄が無いときのみ、レシーバ51に装着されているメモリスティック111に記憶されているコンテンツを、レシーバ51は再生する。なお、ステップS671において、伸張部63とメモリスティック111が、相互認証し、メモリスティック111は、コンテンツ鍵K c oを伸張部63に直接送信し、伸張部63はコンテンツ鍵K c oを受信するようにしてもよい。

【0284】

続いて、ユーザネットワーク5が図30の構成を有し、暗号化されている検査値が記憶部135に記憶されているときの、レシーバ51に装着されている鍵データ143に記憶されているコンテンツを、レシーバ51が再生する処理を、図74のフローチャートを参照して説明する。ステップS701乃至ステップS705の処理は、図73のステップS671乃至ステップS675の処理とそれぞれ同様なので、その説明は省略する。

【0285】

ステップS706において、メモリスティック111の復号部136は、コンテンツ鍵Kcoを記憶している鍵データブロックに対応する検査値を記憶部135が記憶する検査用鍵Kchで復号する。ステップS707において、データ検査部131は、ステップS705で得られたハッシュ値と、ステップS706で復号された検査値とを比較し、一致するか否かを判定し、一致すると判定された場合、その鍵データブロックのデータは改竄されていないので、ステップS708に進む。

【0286】

ステップS708乃至ステップS720の処理は、図73のステップS677乃至ステップS689の処理とそれぞれ同様なので、その説明は省略する。

【0287】

ステップS707において、ステップS705で得られたハッシュ値と、ステップS706で復号された検査値とを比較し、一致しないと判定された場合、その鍵データブロックのデータは改竄されているので、処理は終了する。

【0288】

以上のように、暗号化されている検査値が記憶部135に記憶されているときも、鍵データブロックの改竄が無いときのみ、レシーバ51に装着されているメモリスティック111に記憶されているコンテンツを、レシーバ51は再生する。

【0289】

なお、コンテンツは、音楽データを例に説明したが、音楽データに限らず、動

画像データ、静止画像データ、文書データ、またはプログラムデータでもよい。その際、圧縮は、コンテンツの種類に適した方式、例えば、画像であればMPEG(Moving Picture Experts Group)などが利用される。ウォーターマークも、コンテンツの種類に適した形式のウォーターマークが利用される。

【0290】

また、共通鍵暗号は、ブロック暗号であるDESを使用して説明したが、NTT(商標)が提案するFEAL、IDEA(International Data Encryption Algorithm)、または1ビット乃至数ビット単位で暗号化するストリーム暗号などでもよい。

【0291】

さらに、コンテンツおよびコンテンツ鍵 K_c の暗号化は、共通鍵暗号方式を利用するとして説明したが、公開鍵暗号方式でもよい。

【0292】

また、図65のステップS516、図67のステップS557、図69のステップS593、図71のステップS633、図73のステップS673、および図74のステップS703において、レシーバ51は、メモリスティック111に送信するコマンドに、レシーバ51の秘密鍵で暗号化した署名を付して、メモリスティック111に送信し、メモリスティック111は、その署名を検査することにより、不正に対する耐性をより強化するようにしてもよい。

【0293】

さらに、図65乃至図72のコンテンツの移動の処理において、コンテンツ鍵 K_c は、再暗号化され、一時的に記憶された後、削除されるとして説明したが、コンテンツ鍵 K_c を受け取る側が、コンテンツ鍵を記憶する領域がない等の理由により、コンテンツ鍵 K_c を削除し、コンテンツ鍵 K_c を受け取れなかった場合の不都合を回避する為に、コンテンツ鍵 K_c を送る側は、受信完了信号を受信するまで、コンテンツ鍵 K_c を一時的に使用不可(コンテンツ鍵 K_c の状態を示すフラグを定義し、そのフラグを使用する等の処理をする)とし、受信完了信号を受信できなかったときは、そのコンテンツ鍵 K_c を再度、使用できるような処理を行っても良い。

【0294】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【0295】

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【0296】

【発明の効果】

請求項1に記載の情報処理装置、請求項3に記載の情報処理方法、および請求項4に記載の提供媒体によれば、情報の使用の許諾条件を示す情報を生成し、許諾条件を示す情報の認証情報を生成し、認証情報を記憶するようにしたので、情報の使用の許諾条件の書き換えを検出し、対応することができる。

【0297】

請求項5に記載の情報処理装置、請求項9に記載の情報処理方法、および請求項10に記載の提供媒体によれば、情報の利用のときに必要な関連情報の認証情報を生成し、認証情報を記憶し、関連情報から、他の認証情報を生成し、記憶している認証情報との一致を検証し、情報記憶媒体と相互認証するようにしたので、情報の関連情報の書き換えを検出し、対応することができる。

【0298】

請求項11に記載の情報記憶媒体によれば、認証情報生成手段が、情報の利用のときに必要な関連情報の認証情報を生成し、記憶手段が認証情報を記憶し、検証手段が、関連情報から、他の認証情報を生成し、記憶手段が記憶している認証情報との一致を検証し、相互認証手段が、情報処理装置と相互認証するようにしたので、情報の関連情報の書き換えを検出し、対応することができる。

【図面の簡単な説明】

【図1】

EMDのシステムを説明する図である。

【図 2】

EMDサービスセンタ 1 の機能の構成を示すブロック図である。

【図 3】

EMDサービスセンタ 1 の配送用鍵 K d の送信を説明する図である。

【図 4】

EMDサービスセンタ 1 の配送用鍵 K d の送信を説明する図である。

【図 5】

EMDサービスセンタ 1 の配送用鍵 K d の送信を説明する図である。

【図 6】

EMDサービスセンタ 1 の配送用鍵 K d の送信を説明する図である。

【図 7】

ユーザ登録データベースを説明する図である。

【図 8】

コンテンツプロバイダ 2 の機能の構成を示すブロック図である。

【図 9】

サービスプロバイダ 3 の機能の構成を示すブロック図である。

【図 10】

ユーザホームネットワーク 5 の構成を示すブロック図である。

【図 11】

ユーザホームネットワーク 5 の構成を示すブロック図である。

【図 12】

コンテンツおよびコンテンツに付随する情報を説明する図である。

【図 13】

コンテンツプロバイダセキュアコンテナを説明する図である。

【図 14】

コンテンツプロバイダ 2 の証明書を説明する図である。

【図 15】

サービスプロバイダセキュアコンテナを説明する図である。

【図 16】

サービスプロバイダ 3 の証明書を説明する図である。

【図 17】

取扱方針、価格情報、および使用許諾条件情報を示す図である。

【図 18】

シングルコピーおよびマルチコピーを説明する図である。

【図 19】

取扱方針および価格情報を説明する図である。

【図 20】

取扱方針、価格情報、および使用許諾条件情報を説明する図である。

【図 21】

コンテンツおよびコンテンツに付随する情報の他の構成を説明する図である。

【図 22】

サービスプロバイダセキュアコンテナを説明する図である。

【図 23】

取扱方針、取扱制御情報、価格情報、及び使用許諾条件の構成を示す図である。

【図 24】

コンテンツおよびコンテンツに付随する情報の他の構成を説明する図である。

【図 25】

コンテンツプロバイダセキュアコンテナを説明する図である。

【図 26】

サービスプロバイダセキュアコンテナを説明する図である。

【図 27】

EMDサービスセンタ 1 の、ユーザホームネットワーク 5 からの課金情報の受信
のときの動作を説明する図である。

【図 28】

EMDサービスセンタ 1 の利益分配処理の動作を説明する図である。

【図 29】

EMDサービスセンタ 1 の、コンテンツの利用実績の情報を JASRAC に送信する処理の動作を説明する図である。

【図 30】

ユーザホームネットワーク 5 の更に他の実施の形態の構成を示す図である。

【図 31】

外部記憶部 113 の記憶の態様を説明する図である。

【図 32】

記憶モジュール 73 の記憶の態様を説明する図である。

【図 33】

外部記憶部 113 の他の記憶の態様を説明する図である。

【図 34】

記憶モジュール 73 の他の記憶の態様を説明する図である。

【図 35】

鍵データ 143 の記憶の態様を説明する図である。

【図 36】

記憶部 135 の記憶の態様を説明する図である。

【図 37】

鍵データ 143 の他の記憶の態様を説明する図である。

【図 38】

記憶部 135 の他の記憶の態様を説明する図である。

【図 39】

コンテンツの配布の処理を説明するフローチャートである。

【図 40】

コンテンツの配布の処理を説明するフローチャートである。

【図 41】

EMDサービスセンタ 1 がコンテンツプロバイダ 2 へ配送用鍵 K d を送信する処理を説明するフローチャートである。

【図 4 2】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

【図 4 3】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

【図 4 4】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

【図 4 5】

レシーバ 5 1 の EMD サービスセンタ 1 への登録の処理を説明するフローチャートである。

【図 4 6】

SAM の証明書の説明する図である。

【図 4 7】

登録リストを説明する図である。

【図 4 8】

IC カード 5 5 への SAM 6 2 のデータのバックアップの処理を説明するフローチャートである。

【図 4 9】

IC カード 5 5 への SAM 6 2 のデータのバックアップの処理を説明するフローチャートである。

【図 5 0】

新しいレシーバに IC カード 5 5 のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図 5 1】

新しいレシーバに IC カード 5 5 のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図52】

レシーバ51が、従属関係のあるレコーダ53をEMDサービスセンタ1に登録する処理を説明するフローチャートである。

【図53】

レシーバ51がEMDサービスセンタ1から配送用鍵Kdを受け取る処理を説明するフローチャートである。

【図54】

レコーダの配送用鍵Kdの受け取り処理を説明するフローチャートである。

【図55】

コンテンツプロバイダ2がサービスプロバイダ3にコンテンツプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図56】

コンテンツプロバイダ2がサービスプロバイダ3にコンテンツプロバイダセキュアコンテナを送信する他の処理を説明するフローチャートである。

【図57】

サービスプロバイダ3がレシーバ51にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図58】

サービスプロバイダ3がレシーバ51にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図59】

レシーバ51の課金処理を説明するフローチャートである。

【図60】

レシーバ51の適正なサービスプロバイダセキュアコンテナを受信し、課金する処理の詳細を説明するフローチャートである。

【図61】

レシーバ51の適正なサービスプロバイダセキュアコンテナを受信し、課金する処理の詳細を説明するフローチャートである。

【図 6 2】

MDドライブ 5 4 から供給される暗号化されていないコンテンツを、暗号化し、記録する処理の詳細を説明するフローチャートである。

【図 6 3】

レシーバ 5 1 がコンテンツを再生する処理を説明するフローチャートである。

【図 6 4】

レシーバ 5 1 がデコーダ 5 6 にコンテンツを再生させる処理を説明するフローチャートである。

【図 6 5】

レシーバ 5 1 からメモリスティック 1 1 1 にコンテンツを移動する処理を説明するフローチャートである。

【図 6 6】

レシーバ 5 1 からメモリスティック 1 1 1 にコンテンツを移動する処理を説明するフローチャートである。

【図 6 7】

レシーバ 5 1 からメモリスティック 1 1 1 にコンテンツを移動するフローチャートである。

【図 6 8】

レシーバ 5 1 からメモリスティック 1 1 1 にコンテンツを移動するフローチャートである。

【図 6 9】

メモリスティック 1 1 1 からレシーバ 5 1 にコンテンツを移動するフローチャートである。

【図 7 0】

メモリスティック 1 1 1 からレシーバ 5 1 にコンテンツを移動するフローチャートである。

【図 7 1】

メモリスティック 1 1 1 からレシーバ 5 1 にコンテンツを移動する処理を説明するフローチャートである。

【図72】

メモリスティック111からレシーバ51にコンテンツを移動する処理を説明するフローチャートである。

【図73】

メモリスティック111に記憶されているコンテンツをレシーバ51が再生する処理を説明するフローチャートである。

【図74】

メモリスティック111に記憶されているコンテンツをレシーバ51が再生する処理を説明するフローチャートである。

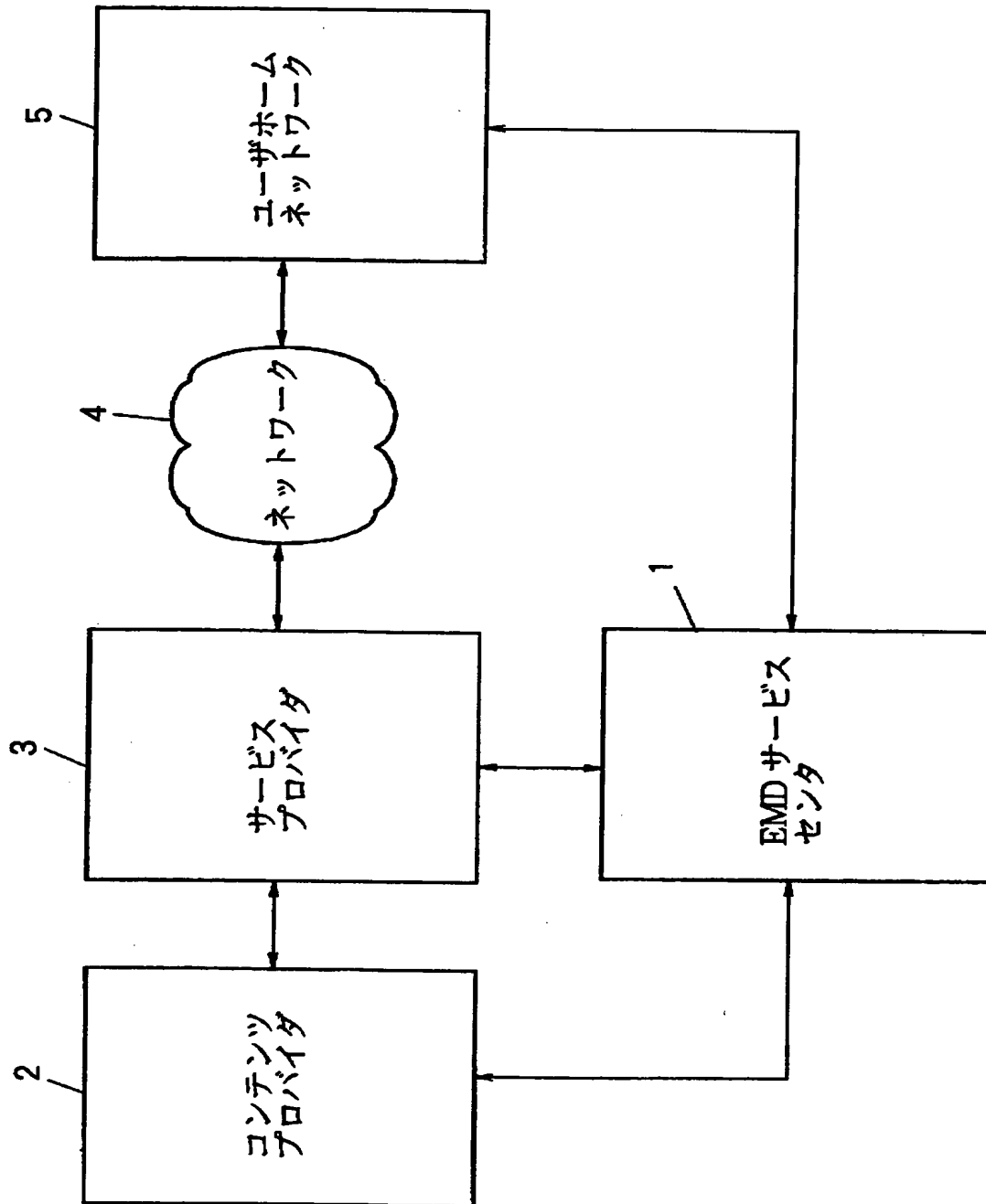
【符号の説明】

1 EMDサービスセンタ, 2 コンテンツプロバイダ, 3 サービスプロバイダ, 5 ユーザホームネットワーク, 16 利益分配部, 18 ユーザ管理部, 42 値付け部, 51 レシーバ, 56 デコーダ, 61 通信部, 62 SAM, 63 伸張部, 71 相互認証モジュール, 72 課金処理モジュール, 73 記憶モジュール, 74 復号/暗号化モジュール, 75 相互認証モジュール, 76 復号モジュール, 77 復号モジュール, 81 相互認証モジュール, 91 復号ユニット, 92 乱数発生ユニット, 93 暗号化ユニット, 101 相互認証モジュール, 102 復号モジュール, 103 復号モジュール, 113 外部記憶部, 114 データ検査モジュール, 121 制御ブロック, 122 情報記憶ブロック, 131 通信部, 132 メモリコントローラ, 133 相互認証部, 134 暗号化部, 135 記憶部, 136 復号部, 137 乱数生成部, 138 データ検査部, 143 鍵データ, 144 暗号化データ

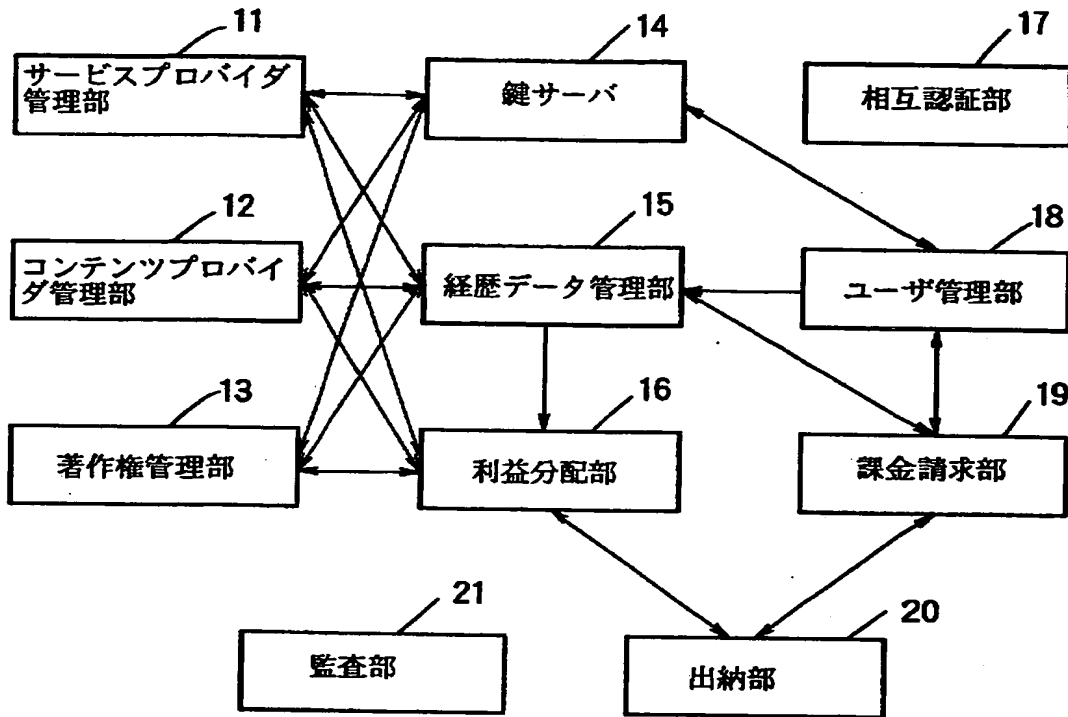
【書類名】

図面

【図 1】

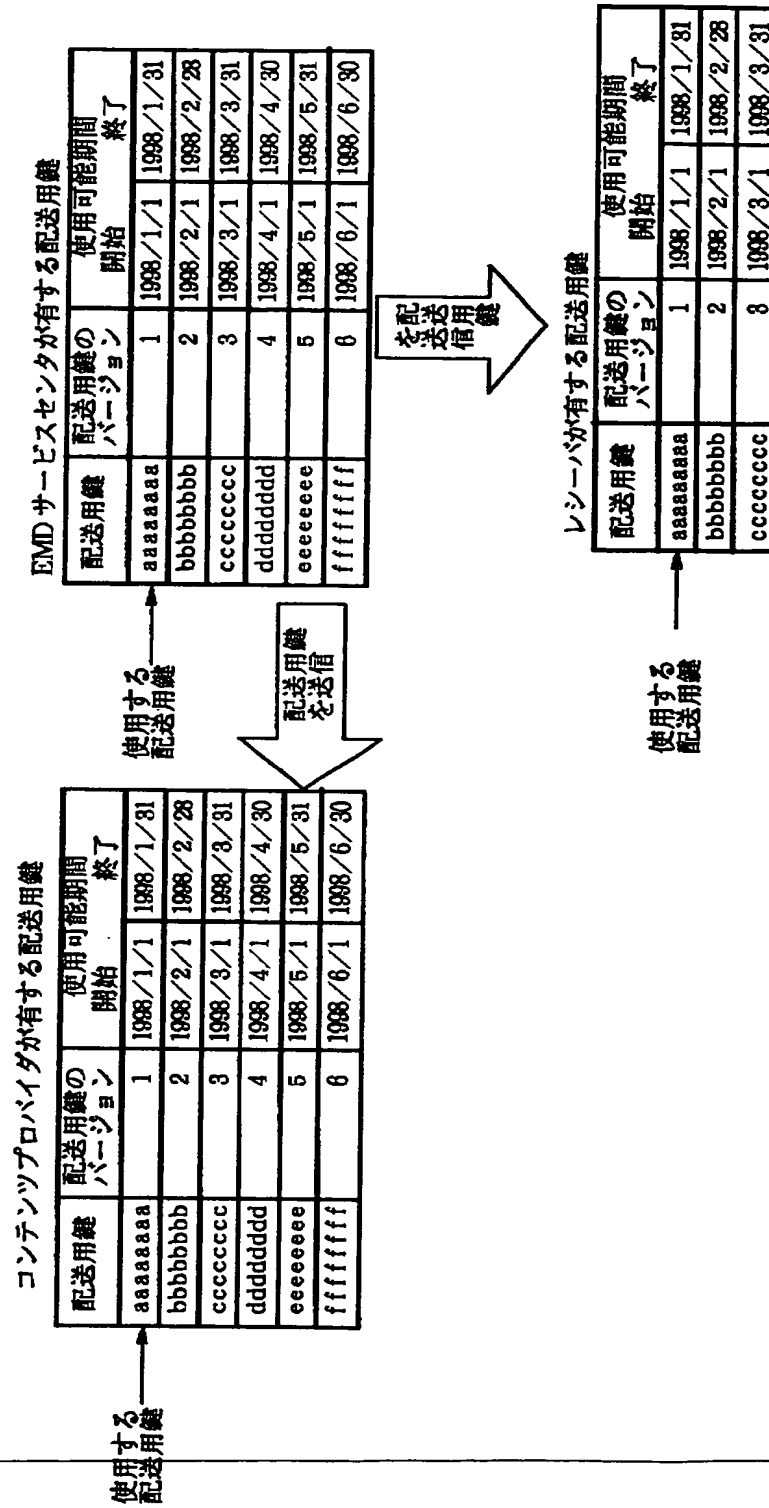


【図 2】

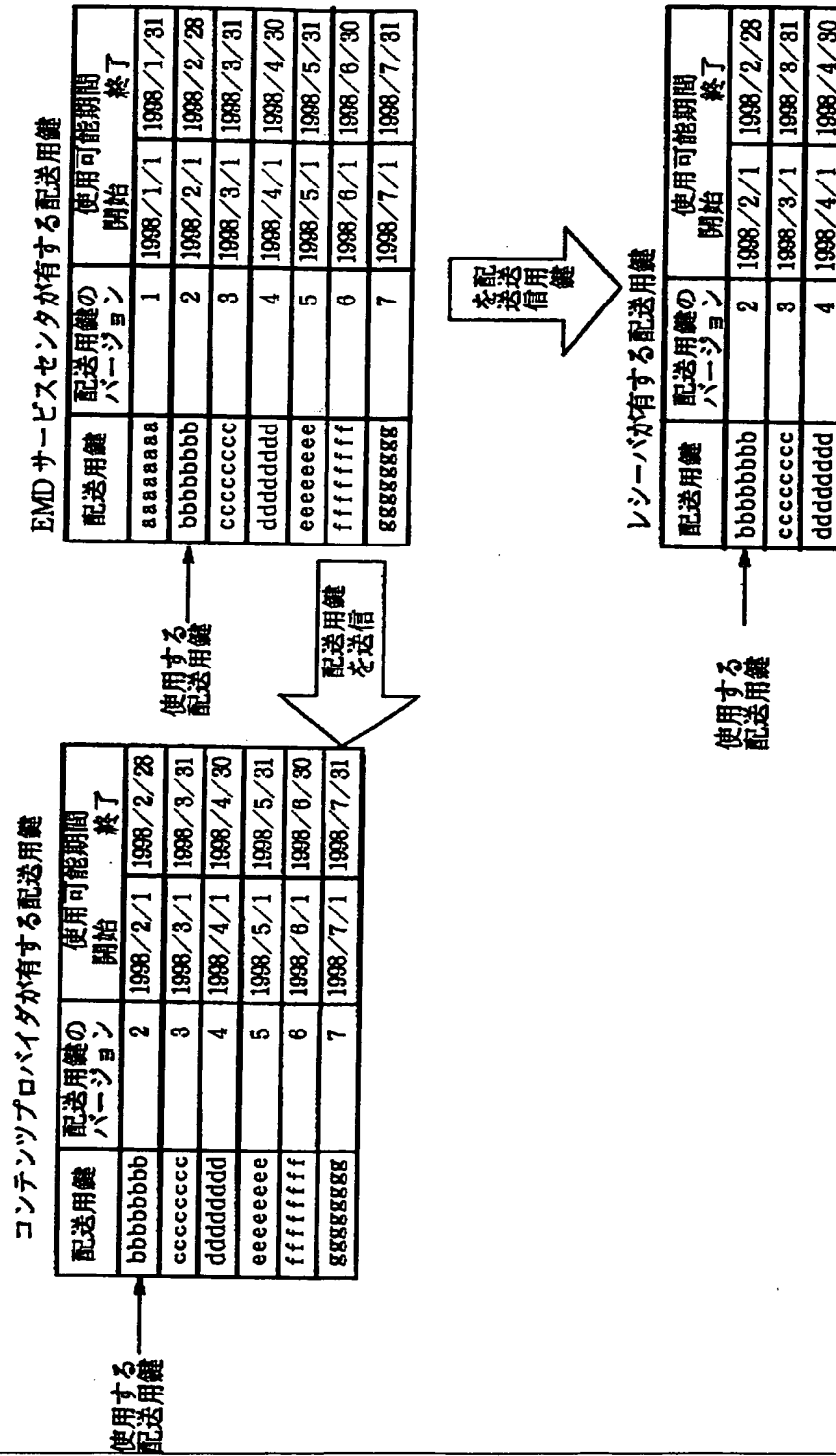


EMD サービスセンタ 1

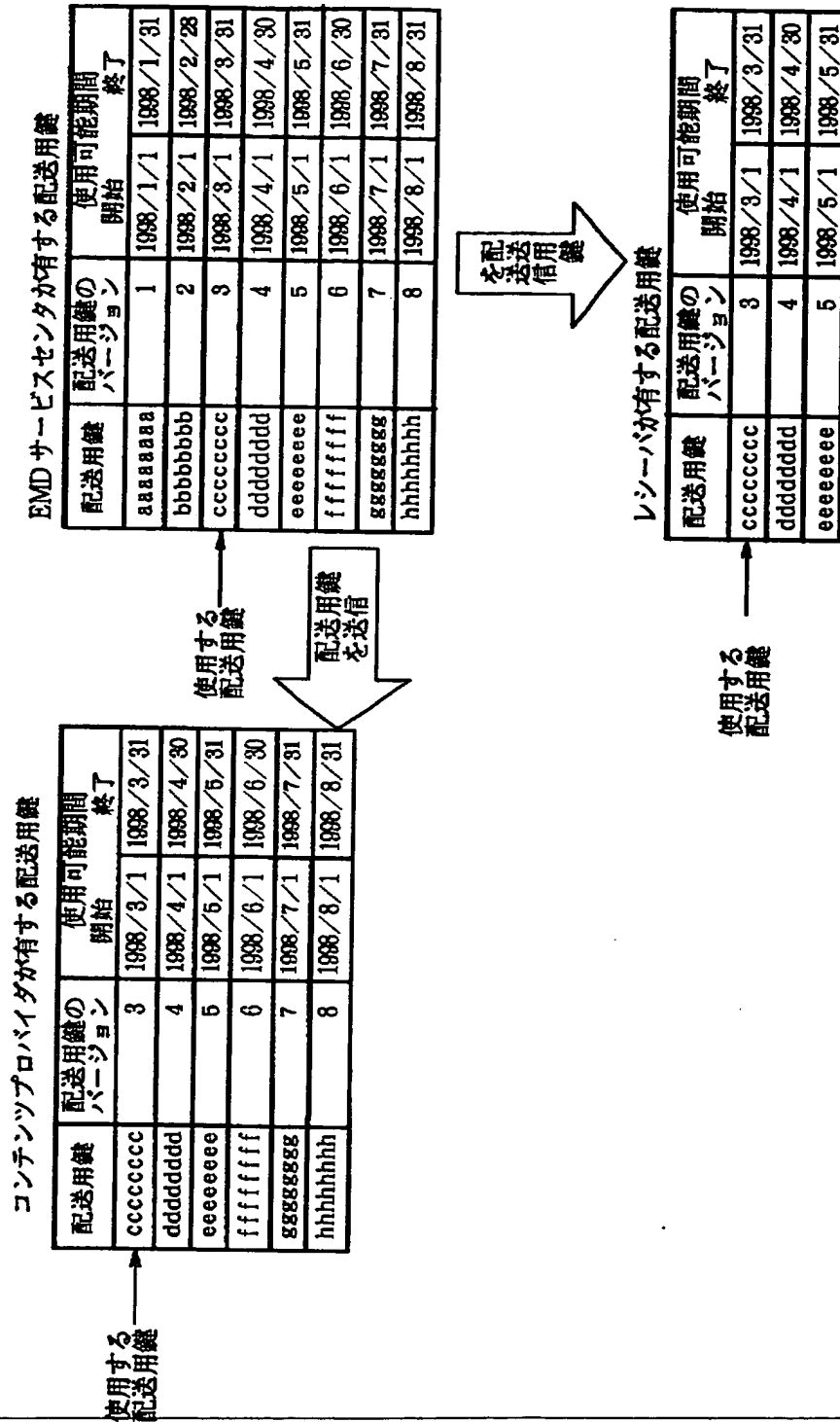
【図3】



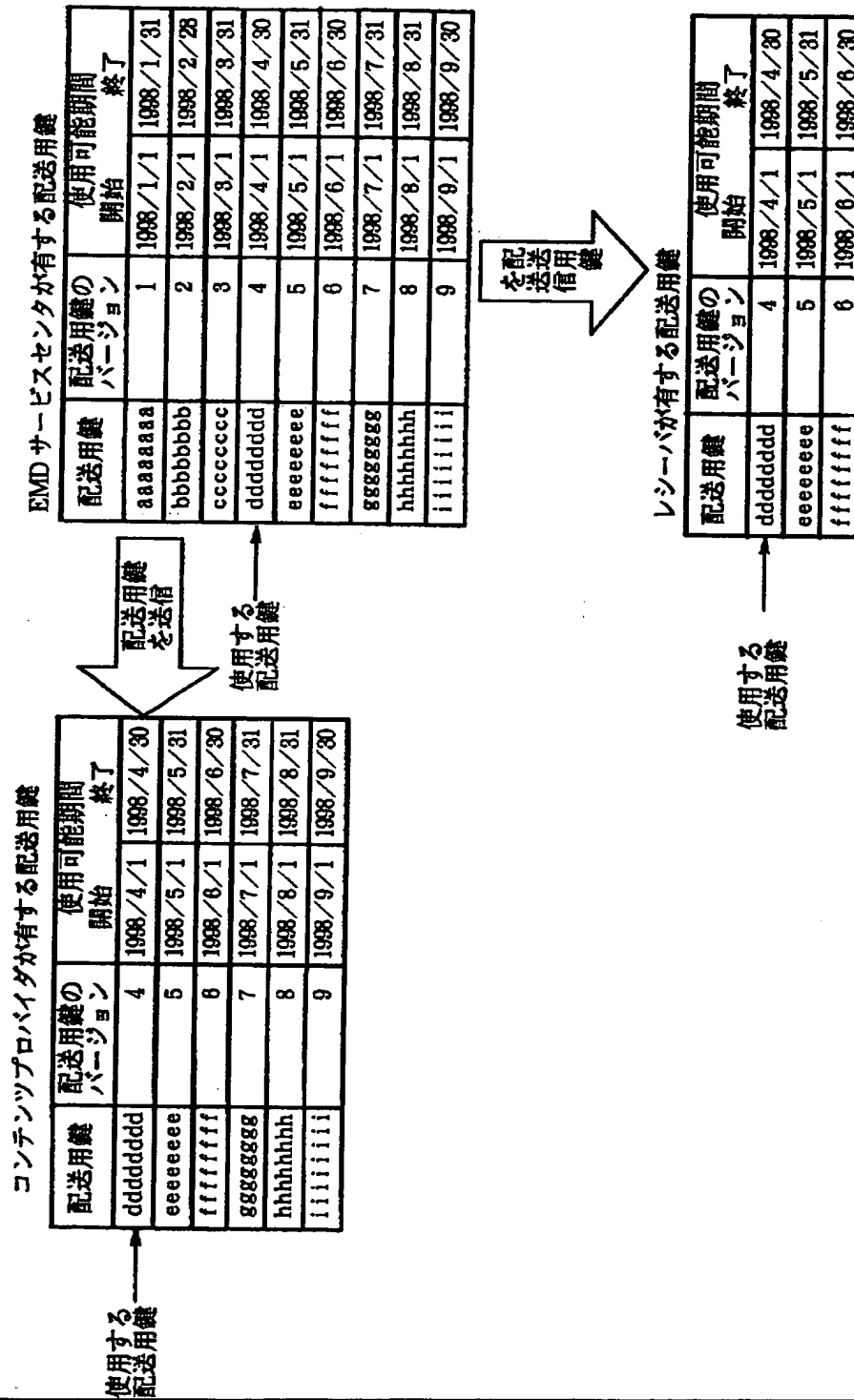
【図 4】



【図 5】



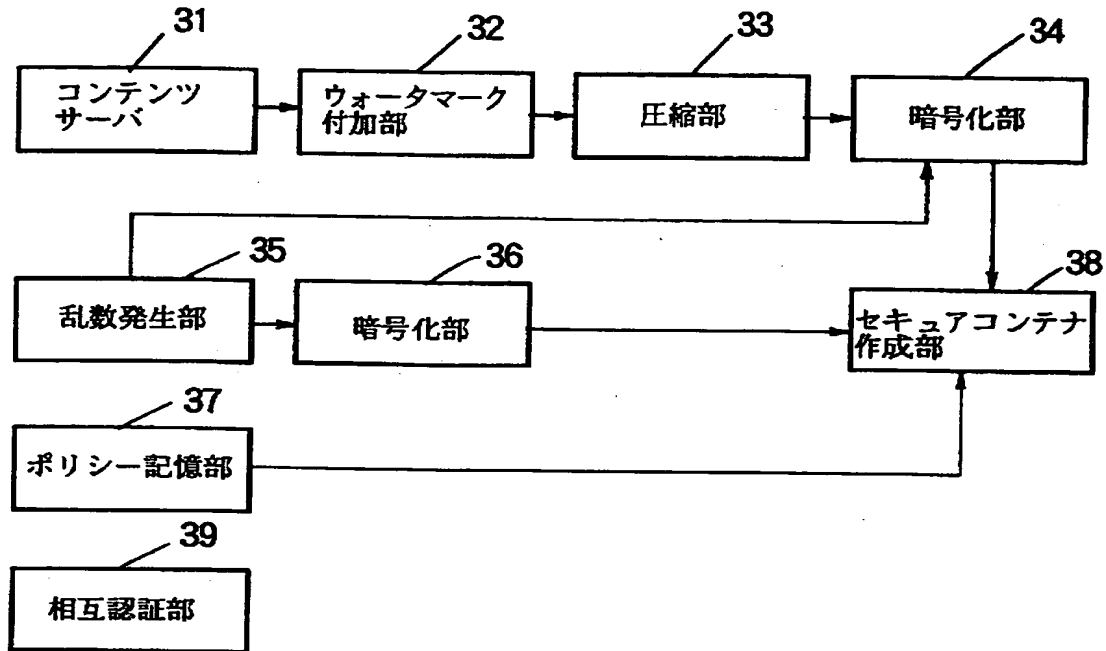
【図 6】



【図 7】

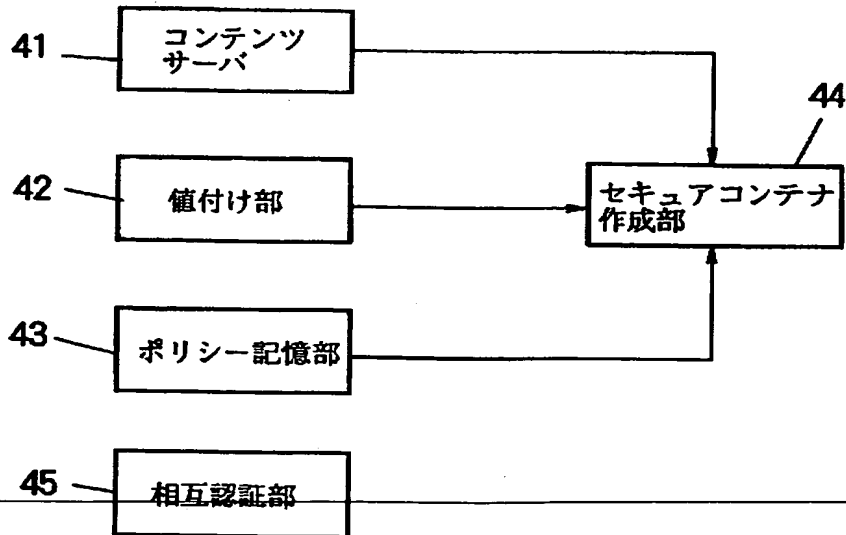
ID	決済処理	登録	EMD サービスセンタとの接続
0000000000000001h	可	可	可
0000000000000002h	可	可	不可
0000000000000003h	可	不可	可
0000000000000004h	可	不可	不可
0000000000000005h	不可	可	可
0000000000000006h	不可	可	不可
0000000000000007h	不可	不可	可
0000000000000008h	不可	不可	不可
0000000000000009h	可	可	可
...			
FFFFFFFFFFFFFFEh	可	不可	不可
FFFFFFFFFFFFFFFh	不可	可	可

【図 8】



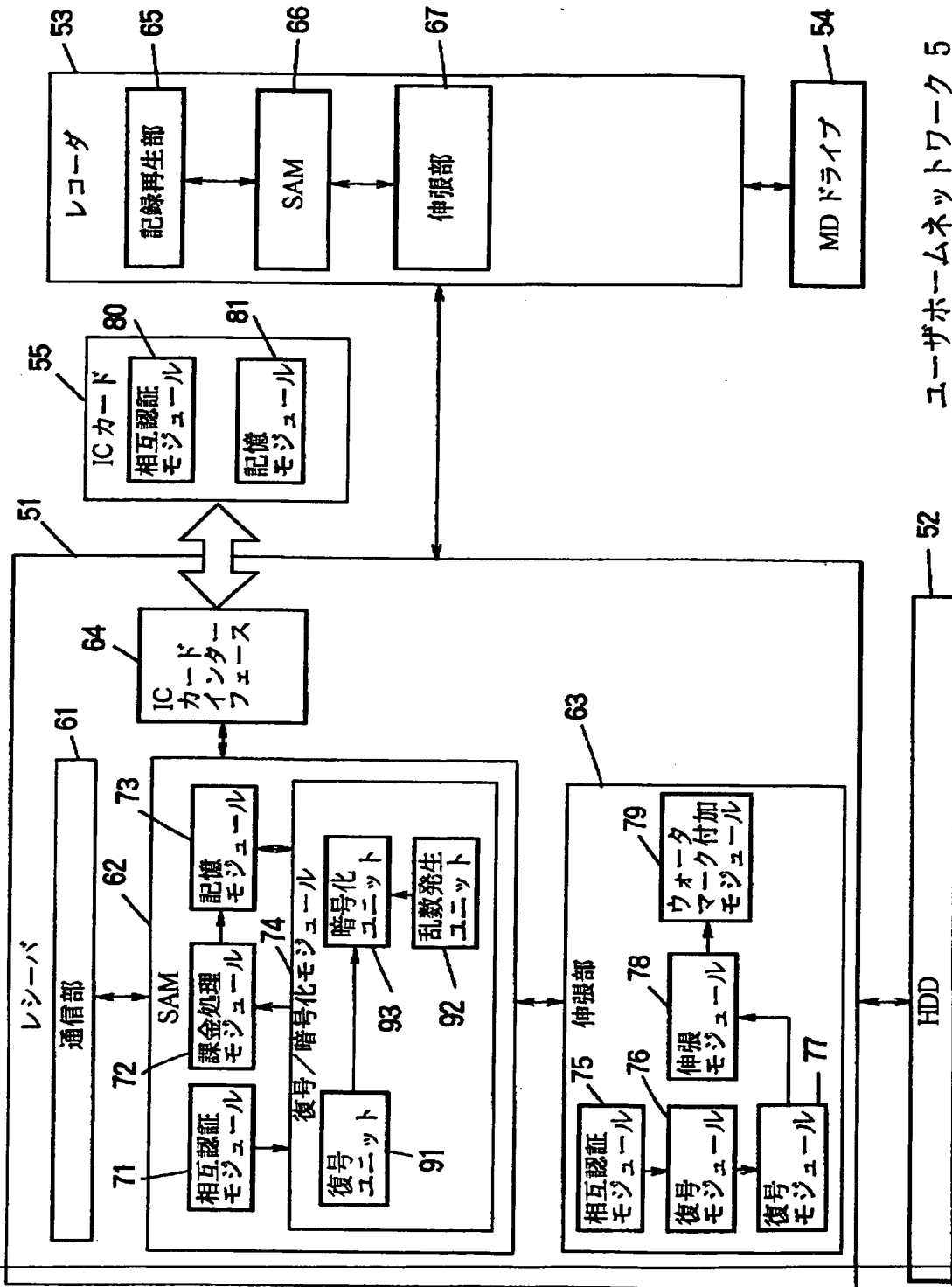
コンテンツプロバイダ 2

【図 9】



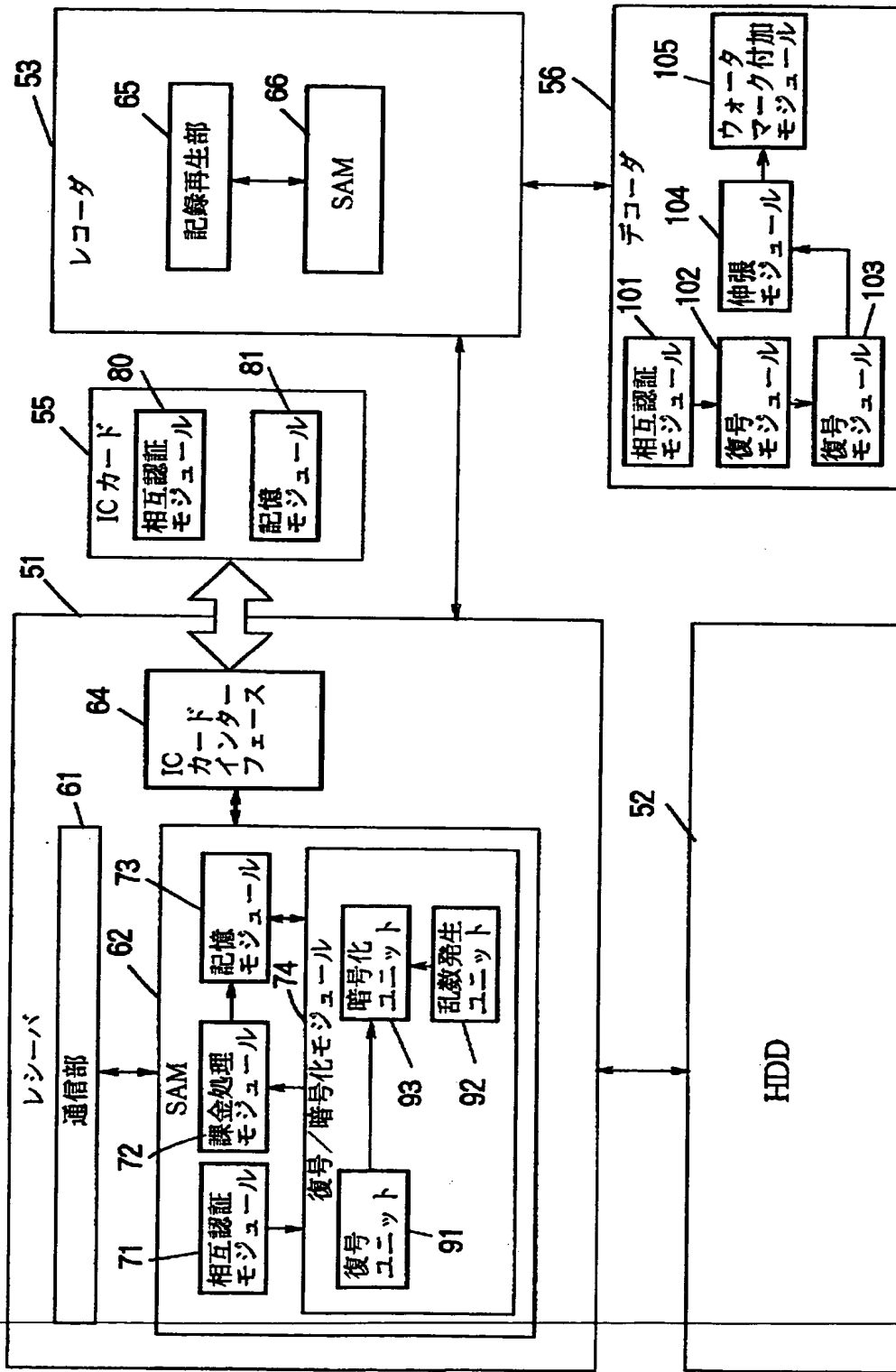
サービスプロバイダ 3

【図10】



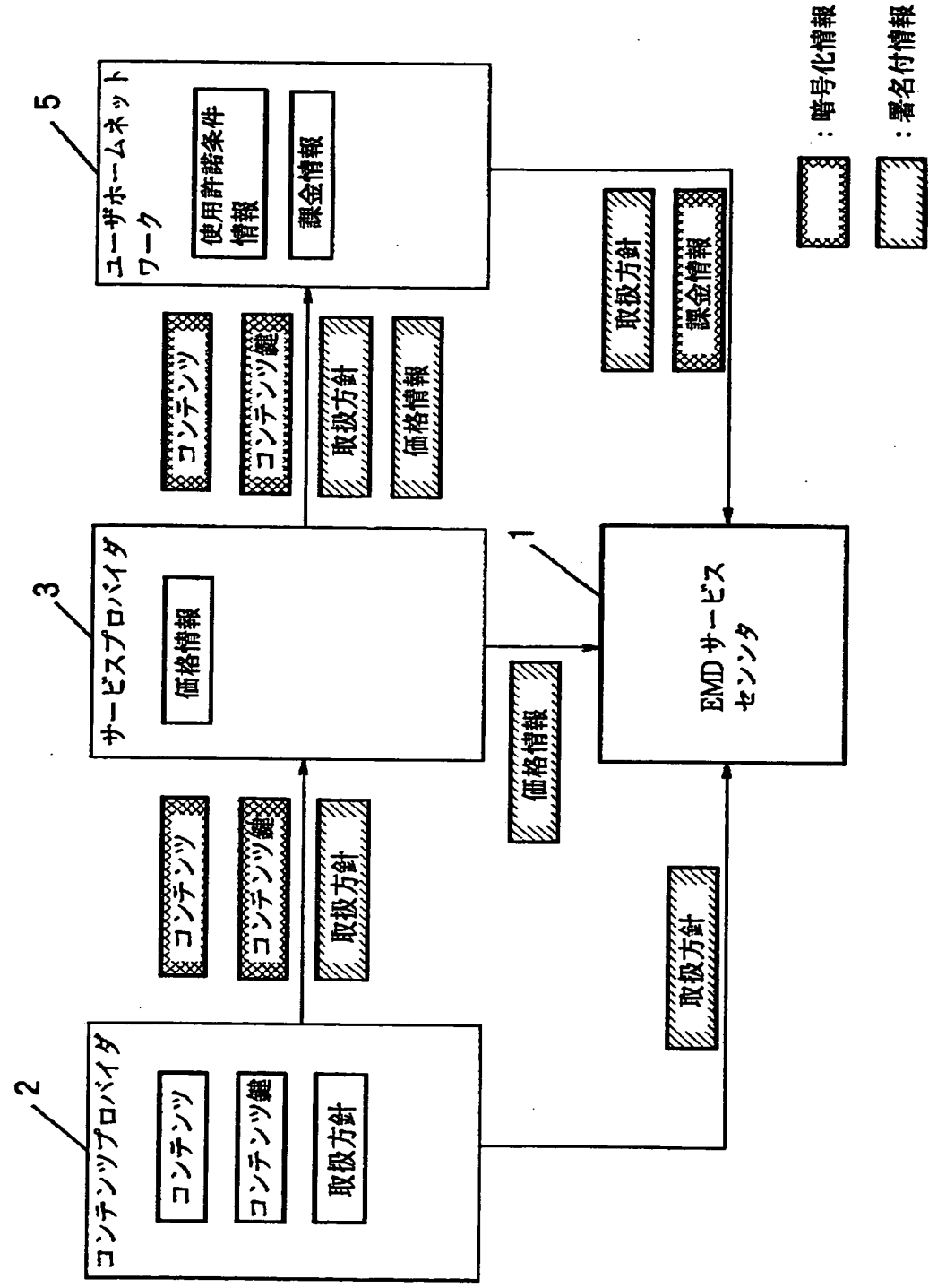
ユーザホームネットワーク 5

【図11】

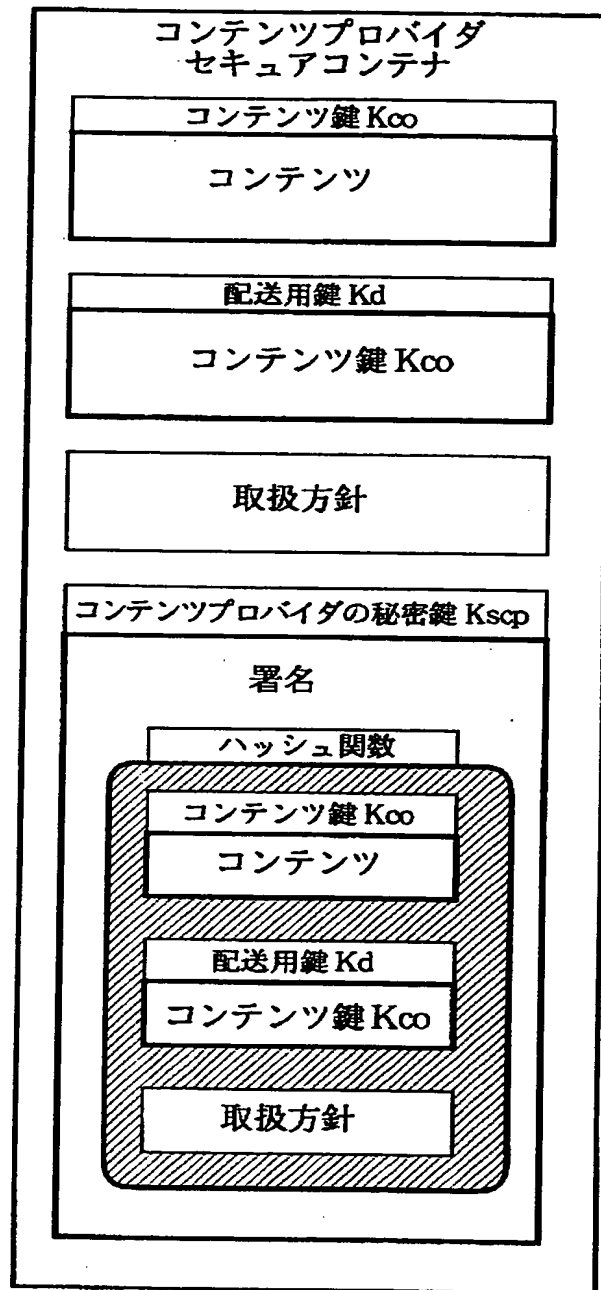


ユーザホームネットワーク 5

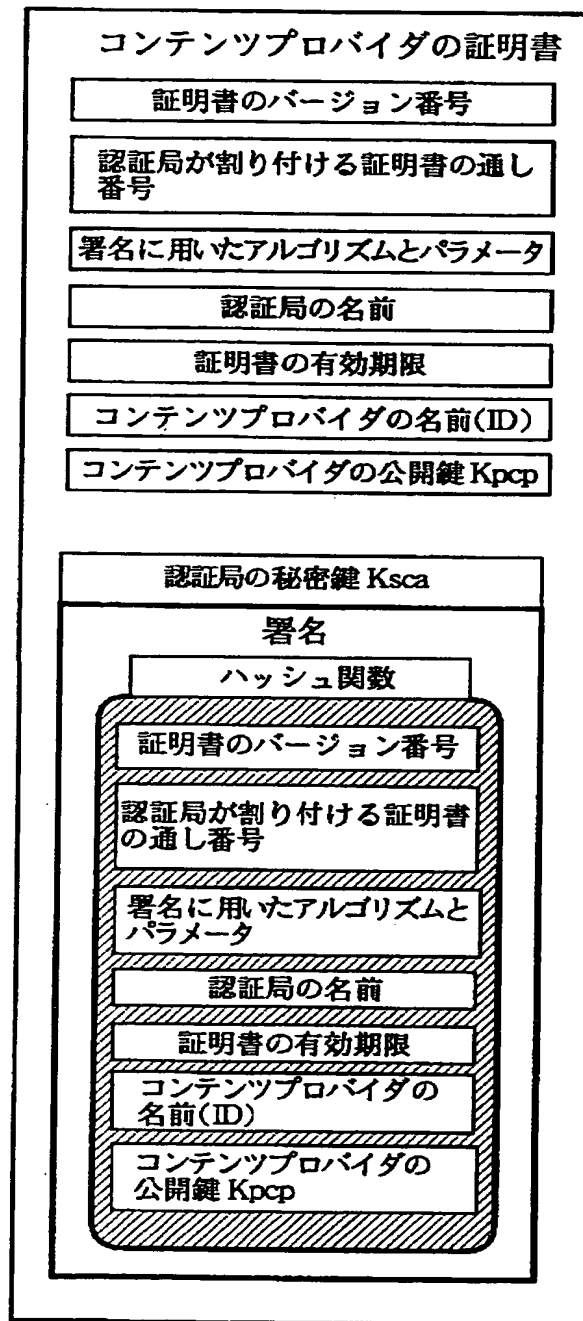
【図12】



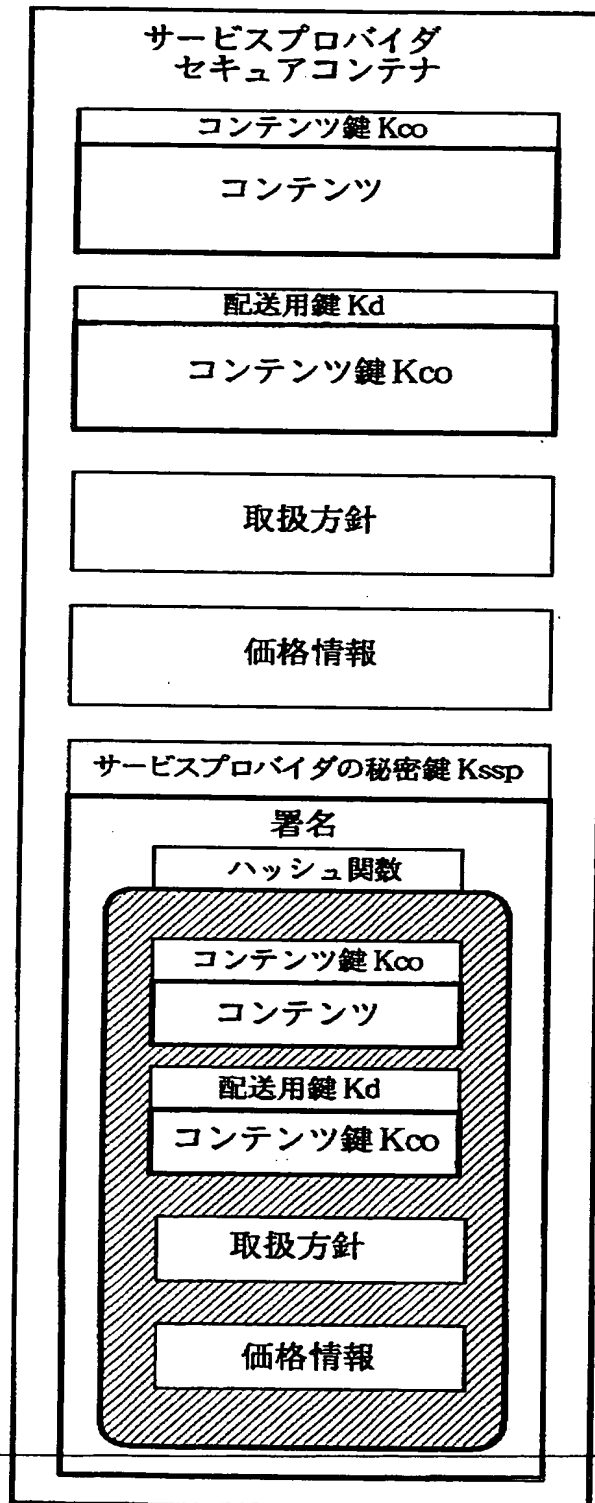
【図 13】



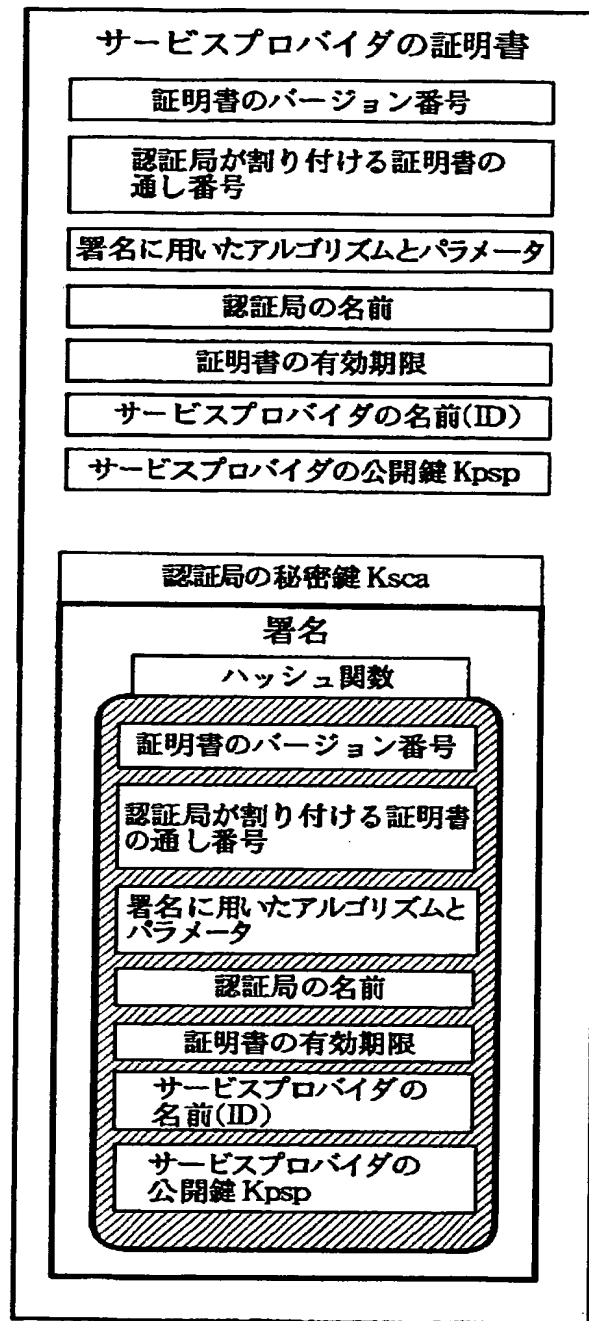
【図 14】



【図 15】



【図 16】

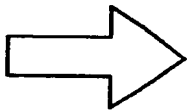


【図 17】

利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	1

取扱方針

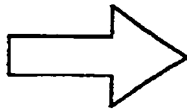
(A)



利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	1
価格	150 円	-	80 円

取扱方針
および
価格情報

(B)

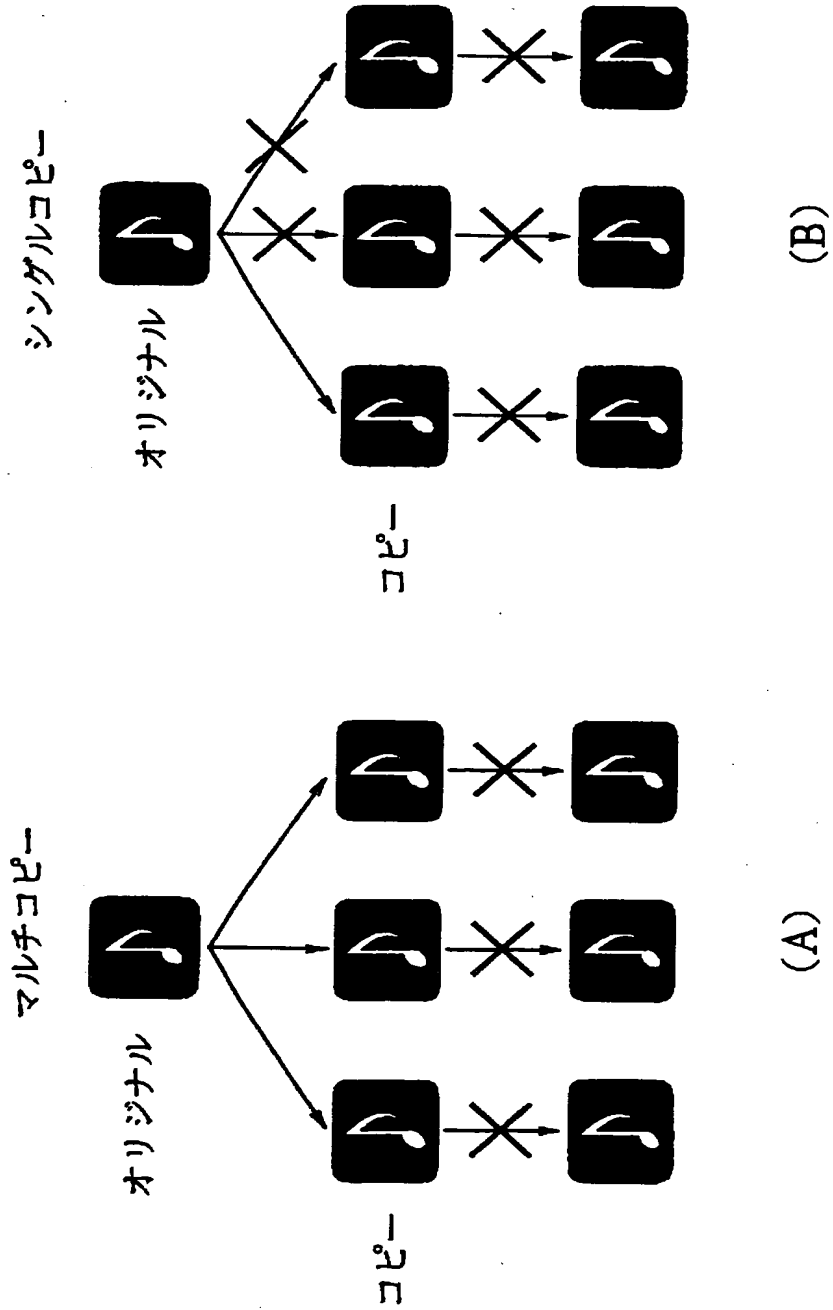


利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	0

使用許諾
条件情報

(C)

【図 18】

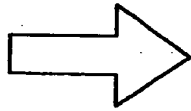


【図 19】

利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	1
利益分配	70 円	-	40 円

取扱方針
利益分配

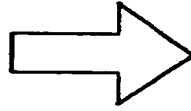
(A)



利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	1
利益分配	60 円	-	30 円
分配価格	150 円	-	80 円

取扱方針
利益分配
価格情報

(B)



利用内容	再生	シングルコピー	マルチコピー
利用回数	1	0	0

課金情報

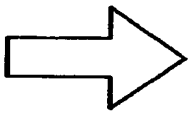
(C)

【図 20】

利用内容	再生		
	制限なし	回数制限	期日制限
	-	5	1988/12/31
価格	-	60 円	80 円

取扱方針
および
価格情報

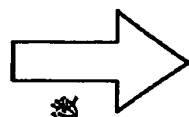
(A)



利用内容	再生		
	制限なし	回数制限	期日制限
	-	5	-

使用許諾条件
情報

(B)



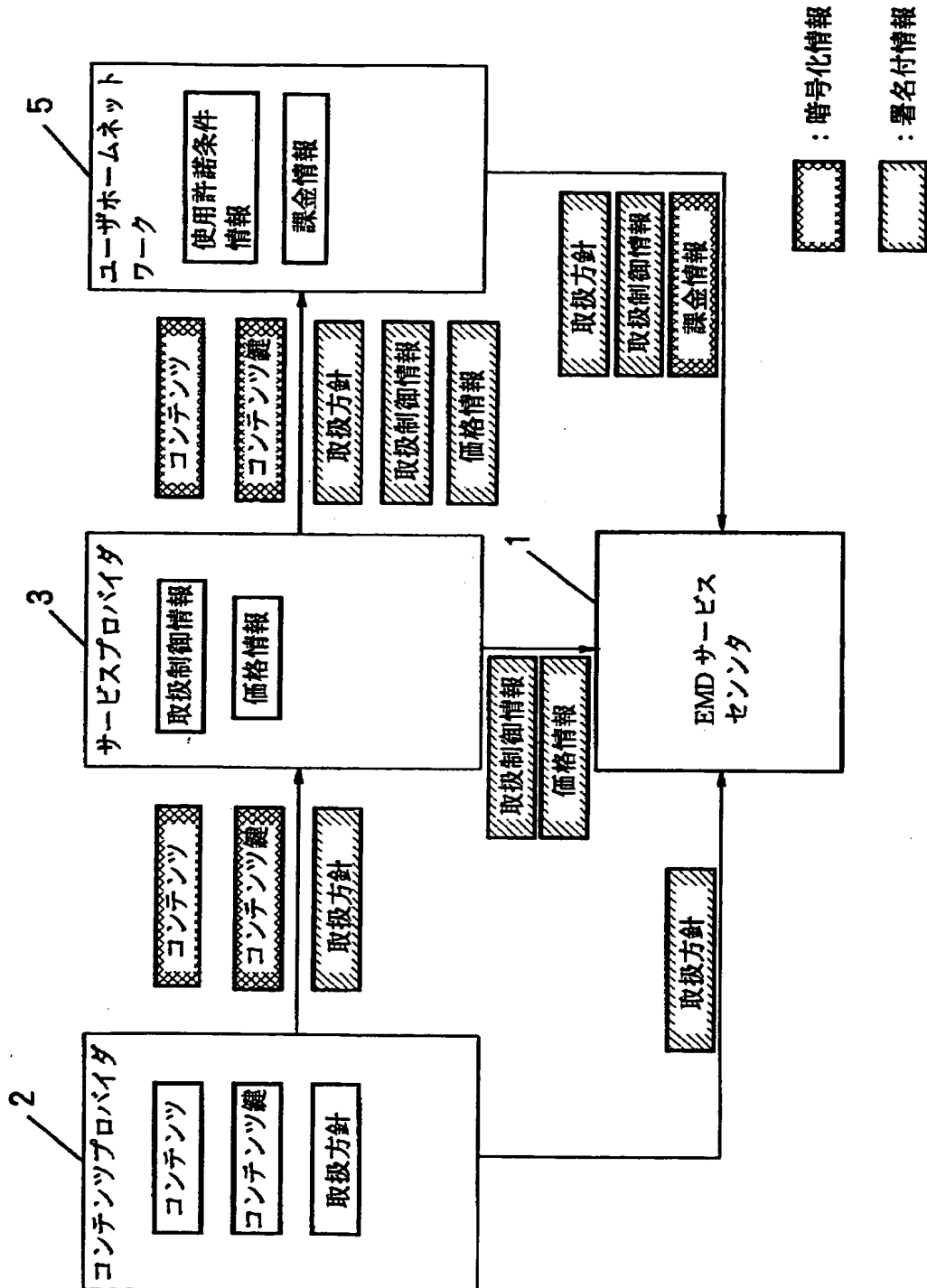
3回再生後

利用内容	再生		
	制限なし	回数制限	期日制限
	-	2	-

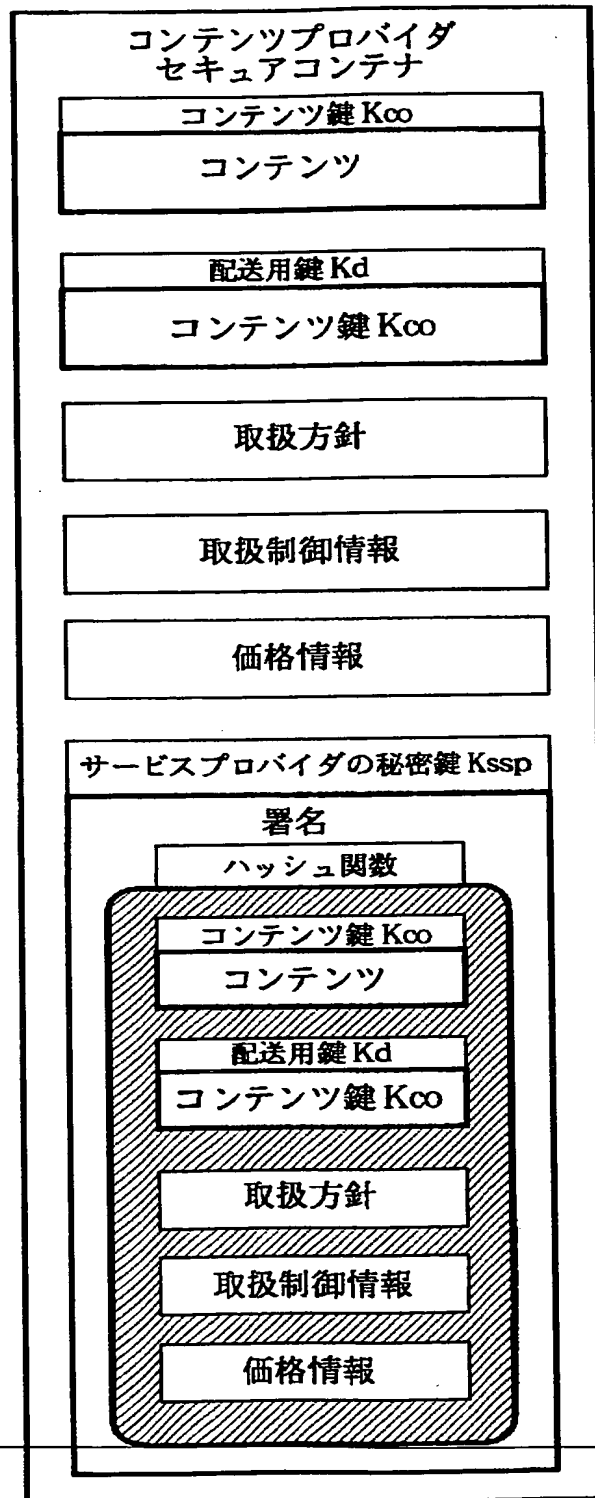
使用許諾条件
情報

(C)

【図 21】



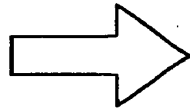
【図 22】



【図 2 3】

(A) 取扱方針

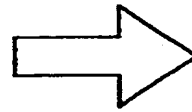
再生: YES; シングルコピー: NO; マルチコピー: YES



利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	1
価格	150 円	-	80 円

取扱制御情報
および
価格情報

(B)

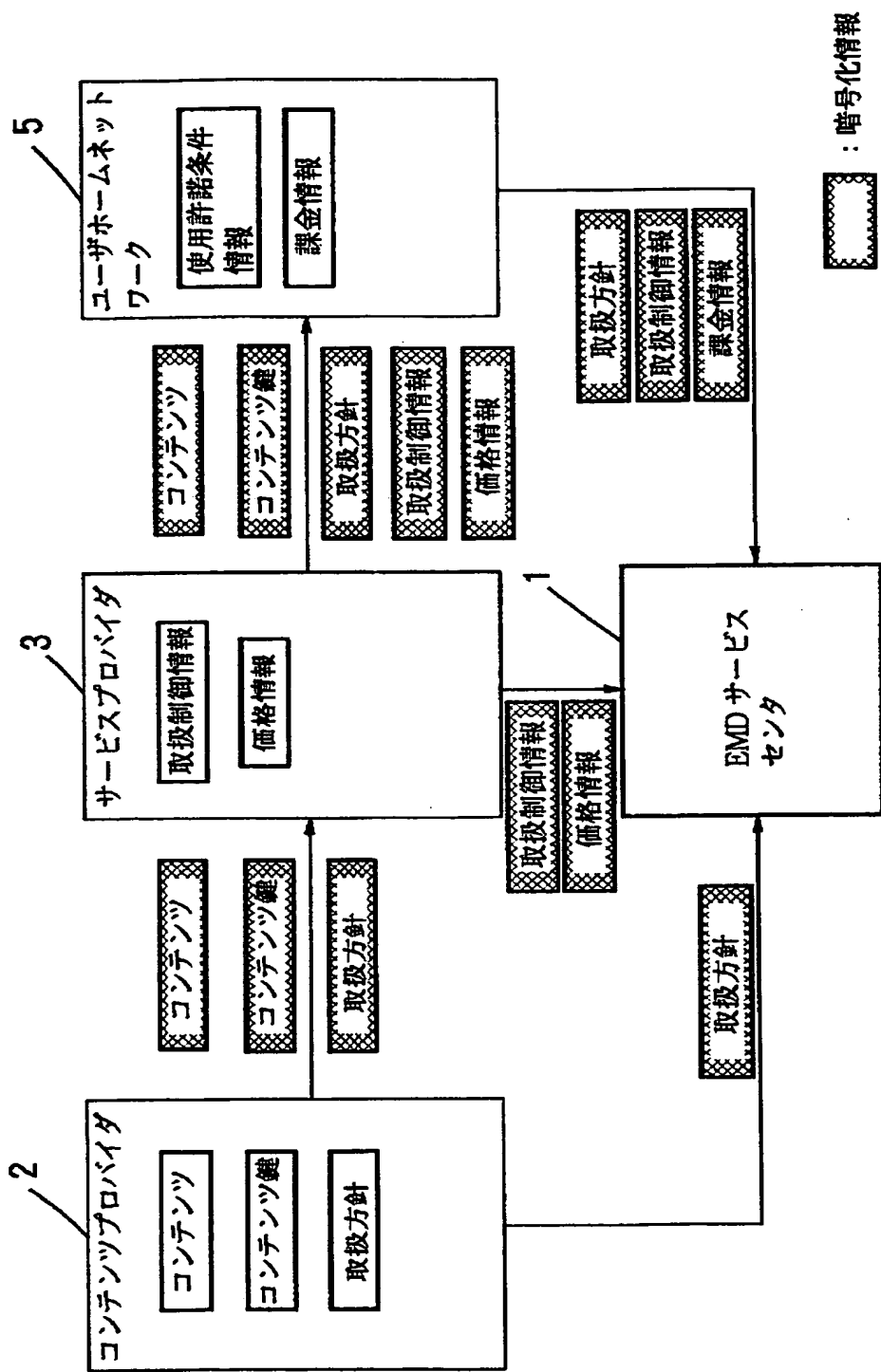


利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	0

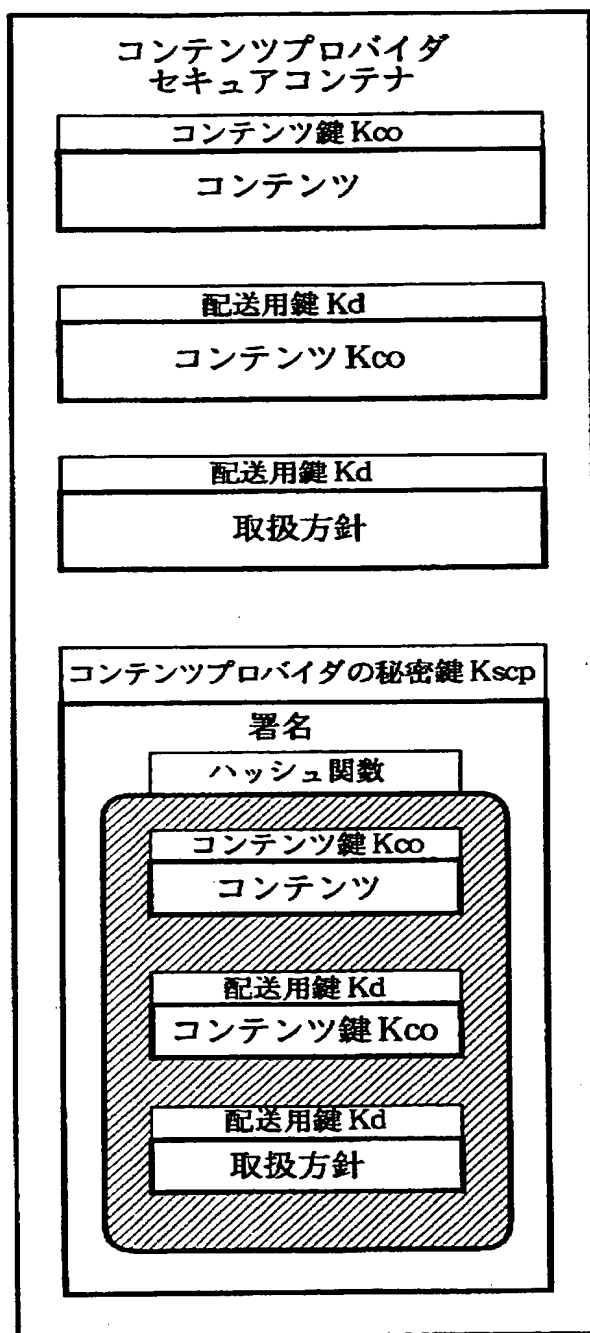
使用許諾
条件情報

(C)

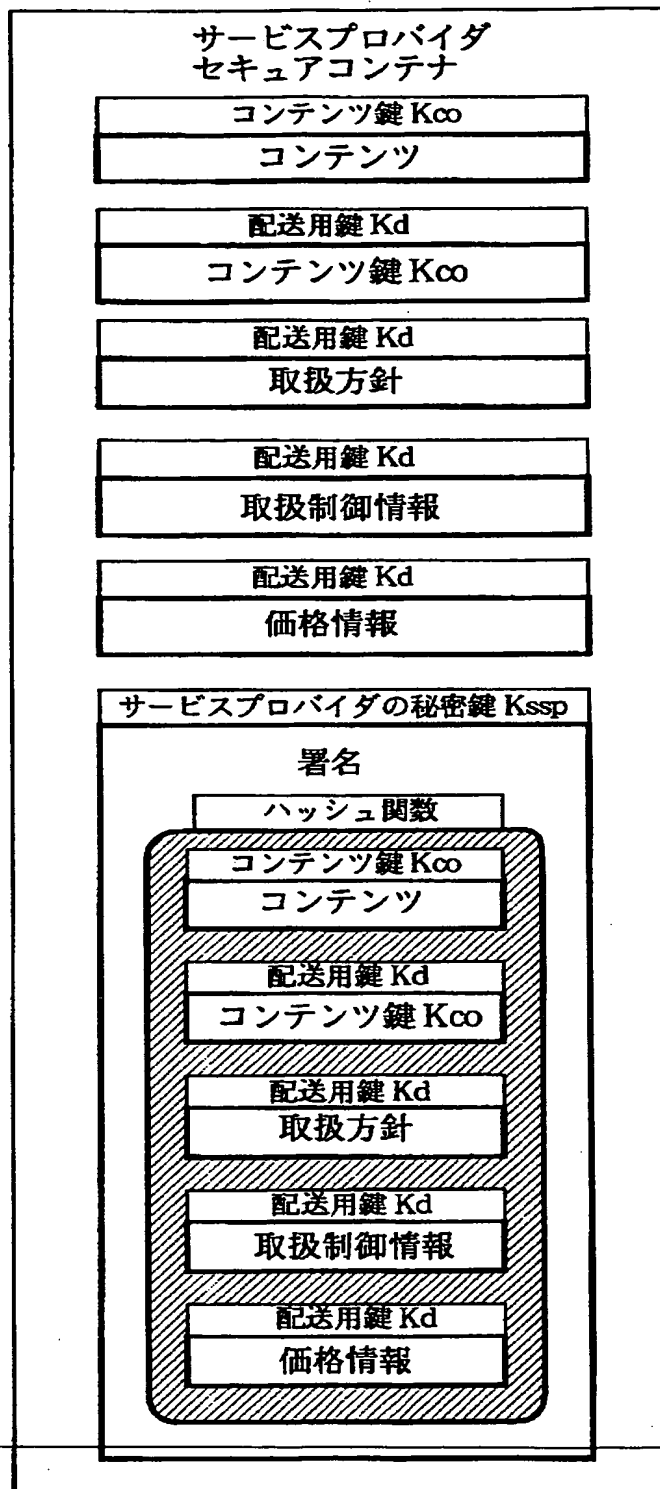
【図 24】



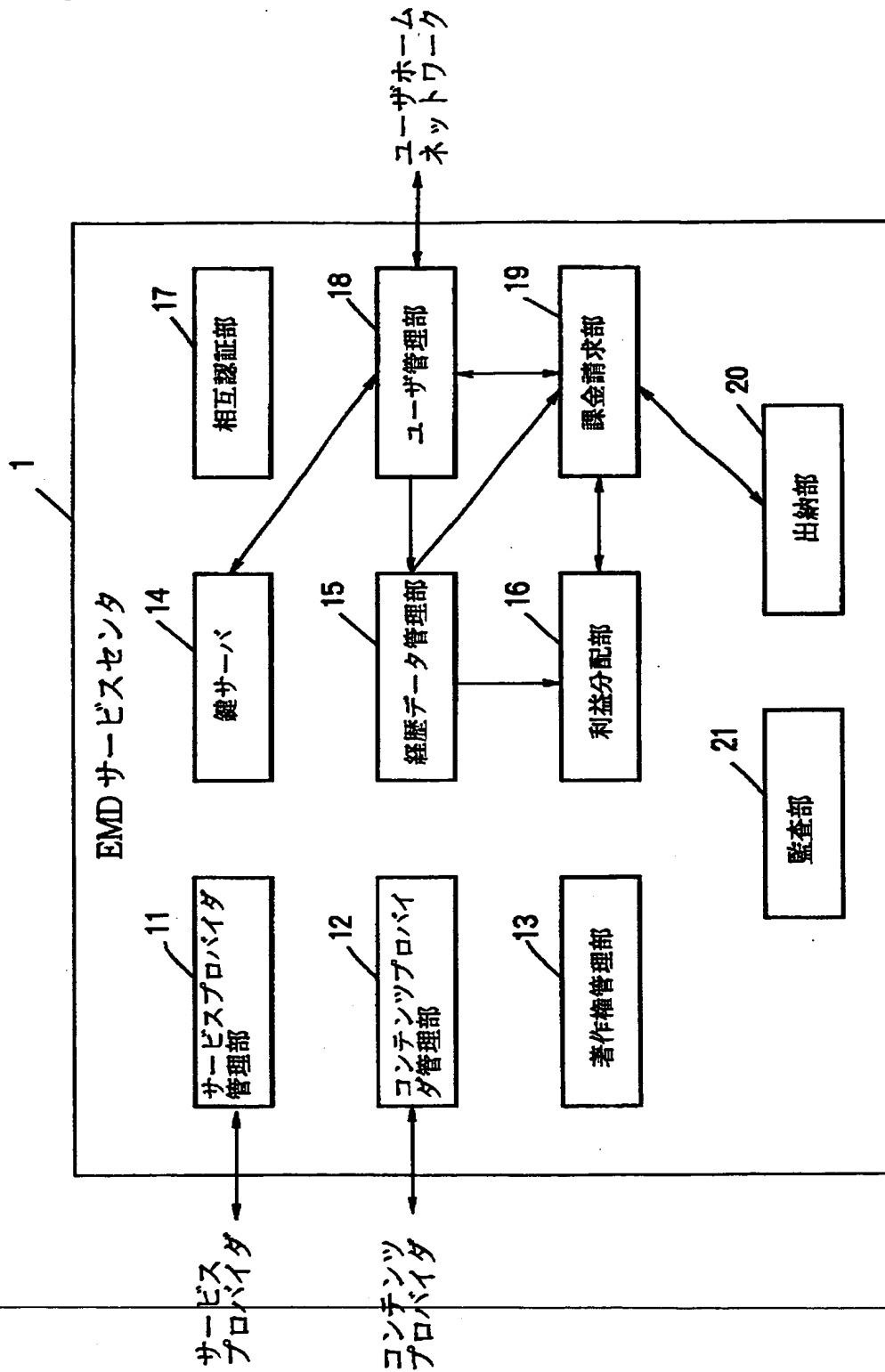
【図 25】



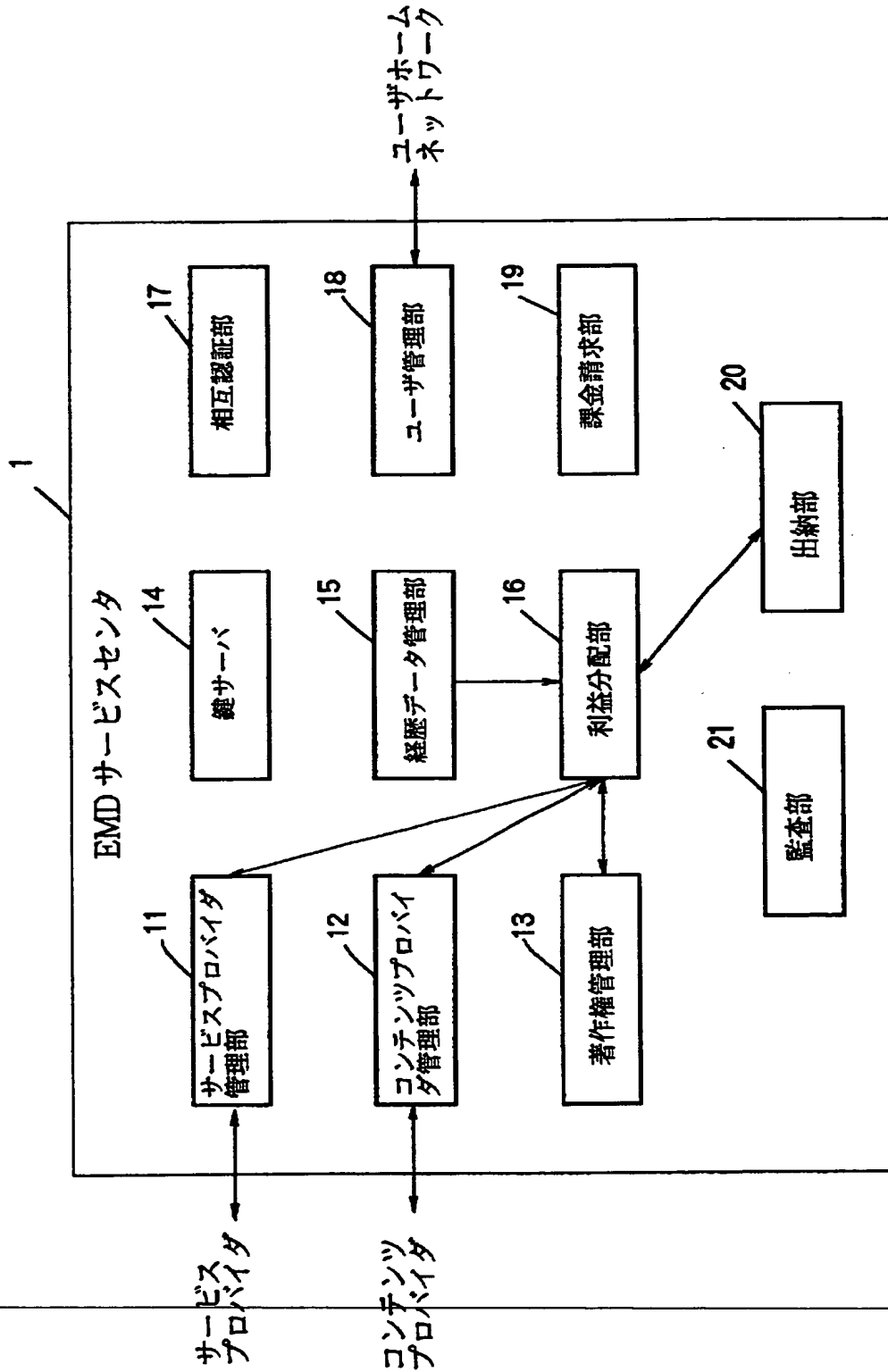
【図 26】



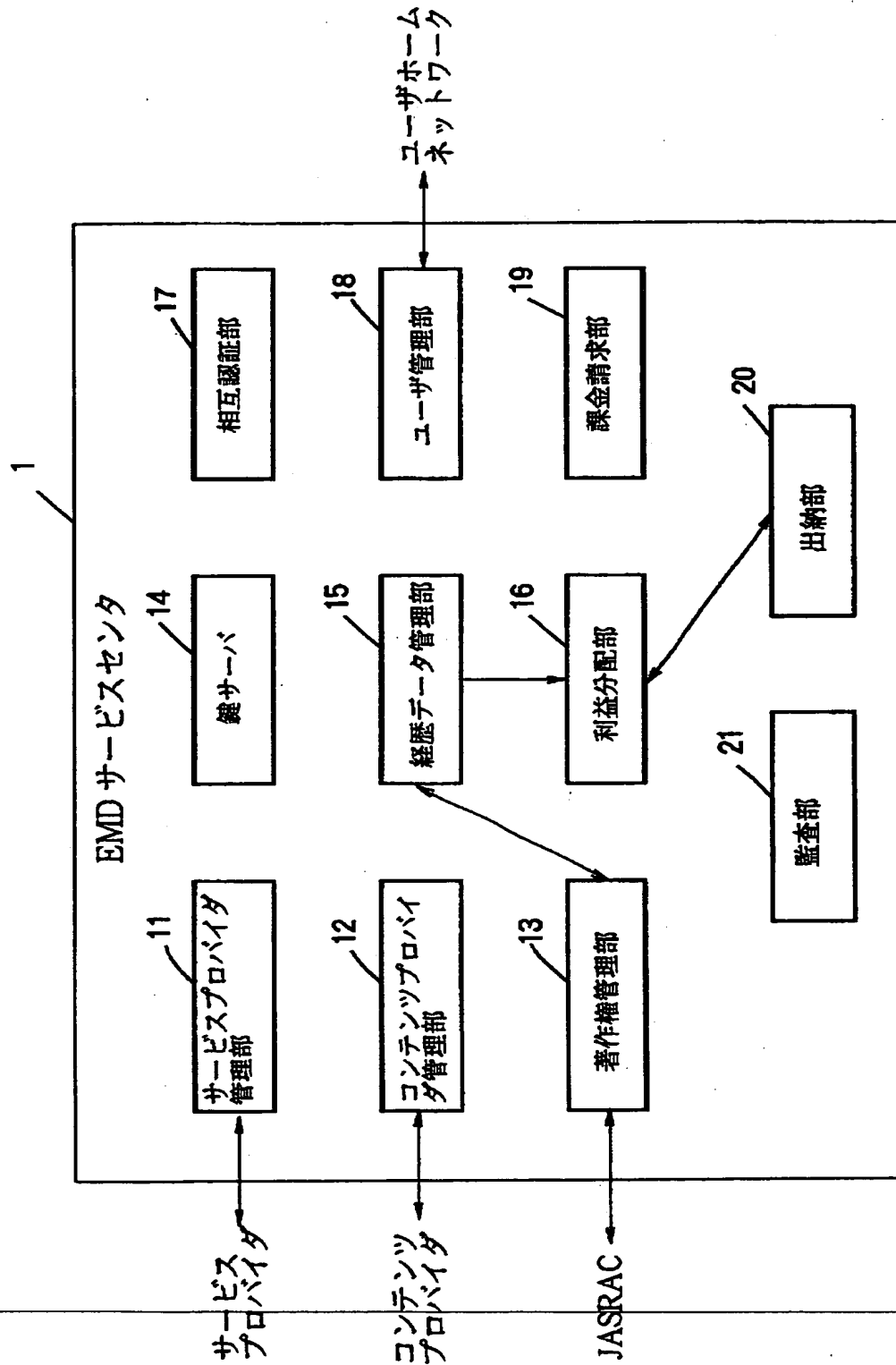
【図 27】



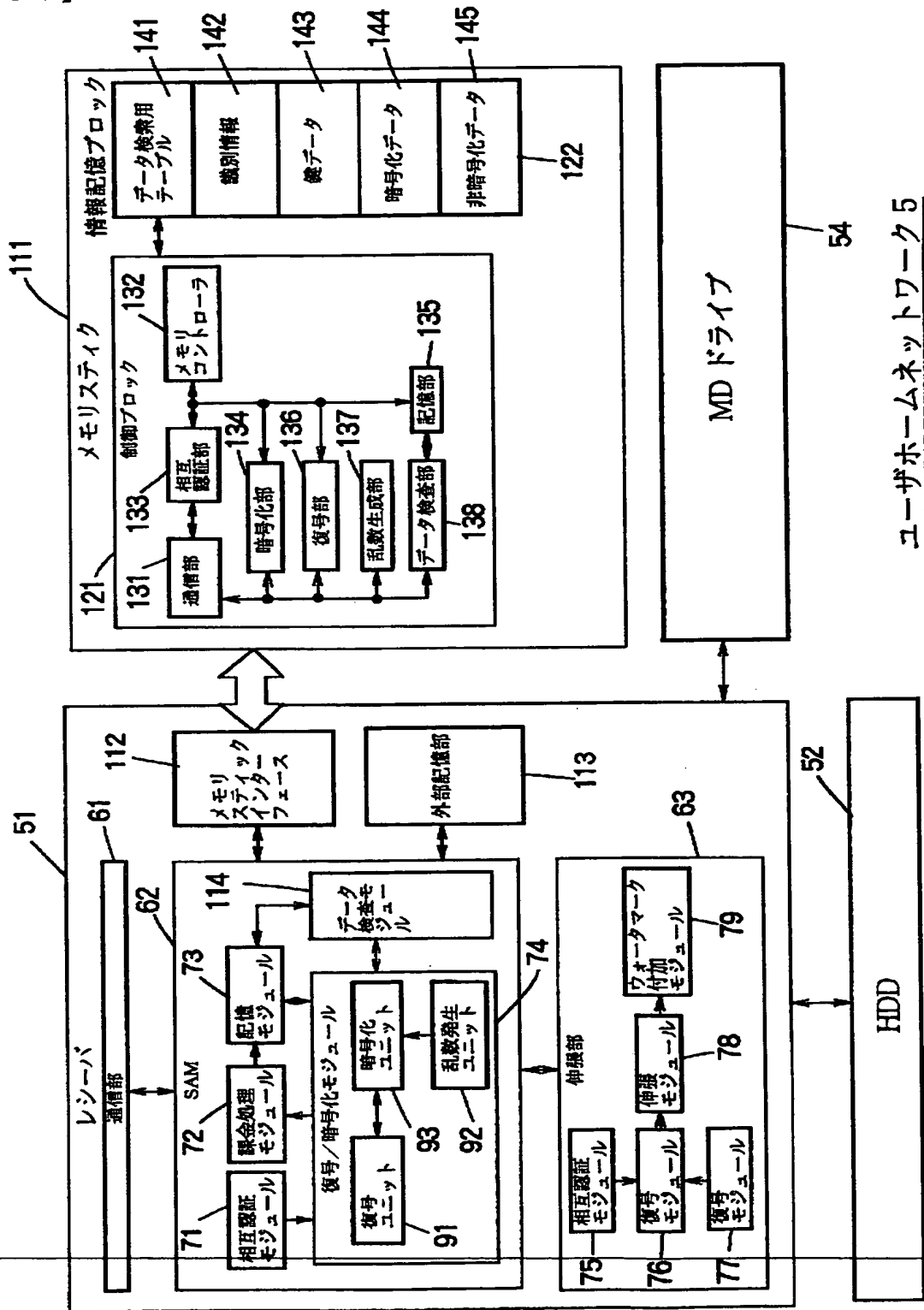
【図 28】



【図29】



【図 30】



【図 3 1】

鍵データブロック 1	コンテンツ鍵 1	コンテンツ ID 1	使用許諾条件情報 1	コンテンツ鍵 2	コンテンツ ID 2	使用許諾条件情報 2
鍵データブロック 2	コンテンツ鍵 3	コンテンツ ID 3	使用許諾条件情報 3	コンテンツ鍵 4	コンテンツ ID 4	使用許諾条件情報 4
鍵データブロック 3	コンテンツ鍵 5	コンテンツ ID 5	使用許諾条件情報 5			
鍵データブロック 4				コンテンツ鍵 6	コンテンツ ID 6	使用許諾条件情報 6
鍵データブロック 5						

【図 3 2】

秘密鍵				
課金情報				
保存用鍵				
配送用鍵				
...				
検査値 1	検査値 2	検査値 3	検査値 4	検査値 5

【図 33】

鍵デ-ータブロック 1	コンテンツ鍵 1	コンテンツ ID 1	使用許諾条件情報 1	コンテンツ鍵 2	コンテンツ ID 2	使用許諾条件情報 2
鍵デ-ータブロック 2	コンテンツ鍵 3	コンテンツ ID 3	使用許諾条件情報 3	コンテンツ鍵 4	コンテンツ ID 4	使用許諾条件情報 4
鍵デ-ータブロック 3	コンテンツ鍵 5	コンテンツ ID 5	使用許諾条件情報 5			
鍵デ-ータブロック 4				コンテンツ鍵 6	コンテンツ ID 6	使用許諾条件情報 6
鍵デ-ータブロック 5						
鍵デ-ータブロック 6						
	検査値 1	検査値 2	検査値 3	検査値 4	検査値 5	検査値 6

【図 34】

秘密鍵
課金情報
保存用鍵
配送用鍵
検査用鍵
...

【図 35】

鍵データブロック 1	コンテンツ鍵 1	コンテンツ ID 1	使用許諾条件情報 1	コンテンツ鍵 2	コンテンツ ID 2	使用許諾条件情報 2
鍵データブロック 2	コンテンツ鍵 3	コンテンツ ID 3	使用許諾条件情報 3	コンテンツ鍵 4	コンテンツ ID 4	使用許諾条件情報 4
鍵データブロック 3	コンテンツ鍵 5	コンテンツ ID 5	使用許諾条件情報 5			
鍵データブロック 4	コンテンツ鍵 6	コンテンツ ID 6	使用許諾条件情報 6			

【図 36】

秘密鍵			
保存用鍵			
...			
検査値 1	検査値 2	検査値 3	検査値 4

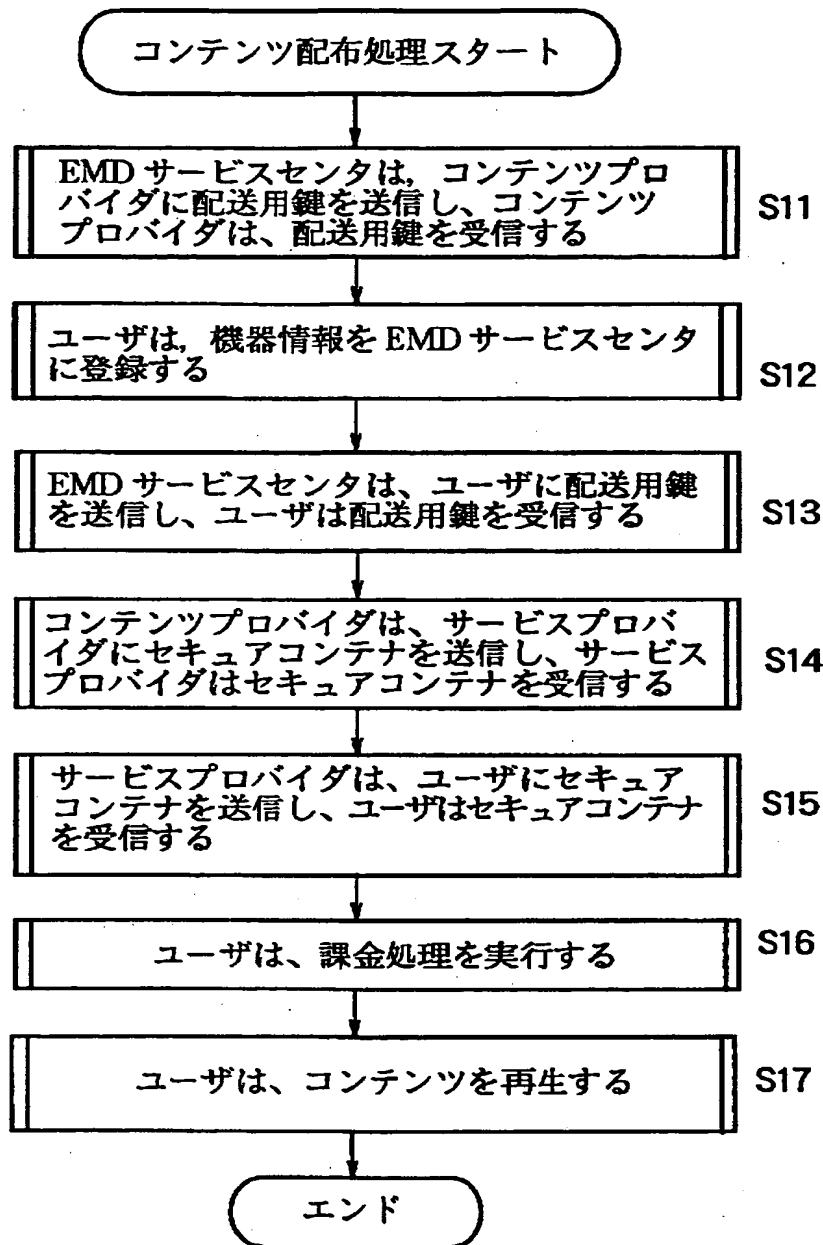
【図37】

鍵データベース1	コンテンツ鍵1	コンテンツID1	使用許諾条件情報1	コンテンツ鍵2	コンテンツID2	使用許諾条件情報2
鍵データベース2	コンテンツ鍵3	コンテンツID3	使用許諾条件情報3	コンテンツ鍵4	コンテンツID4	使用許諾条件情報4
鍵データベース3	コンテンツ鍵5	コンテンツID5	使用許諾条件情報5			
鍵データベース4	コンテンツ鍵6	コンテンツID6	使用許諾条件情報6			
検査値1		検査値2		検査値3	検査値4	

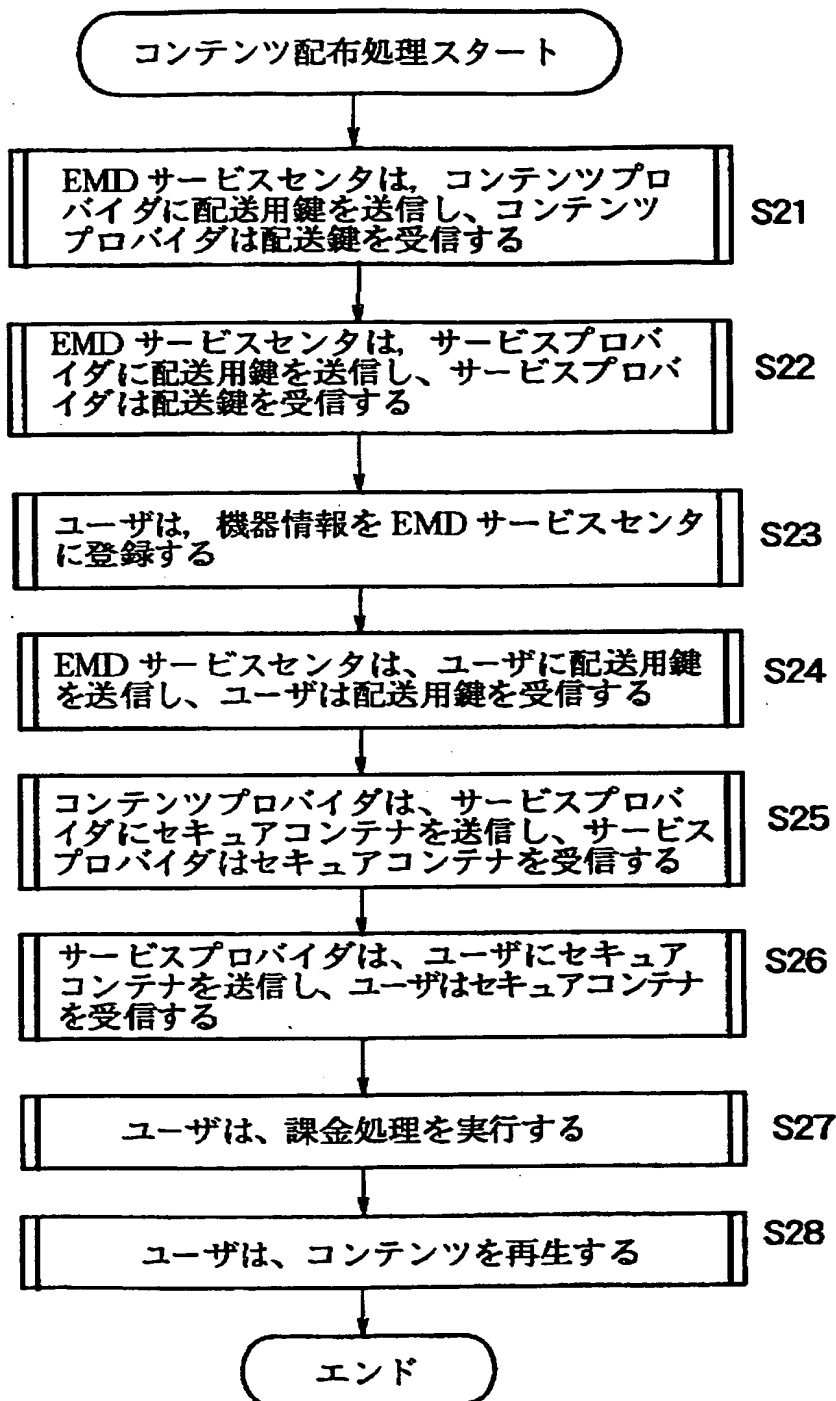
【図 38】

秘密鍵
検査用鍵
保存用鍵
...

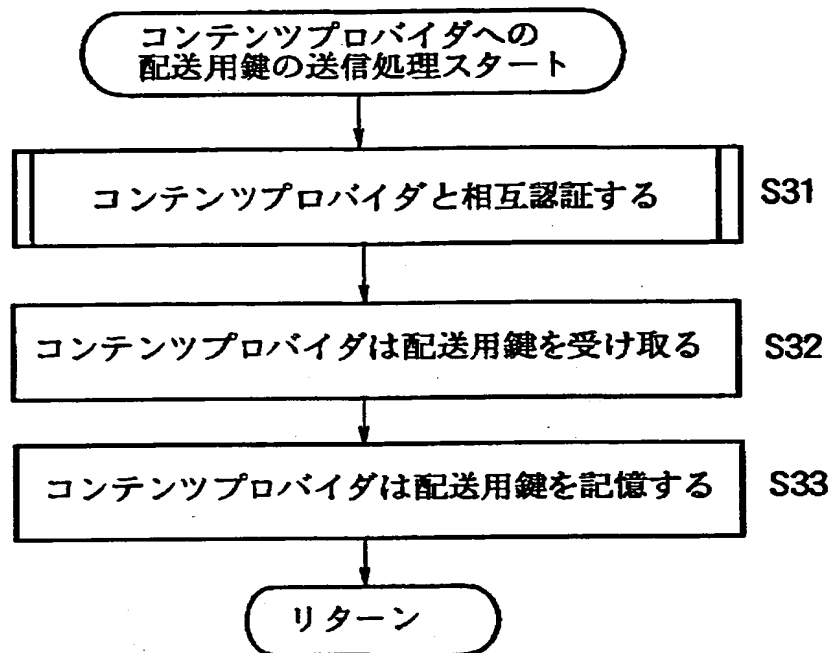
【図 39】



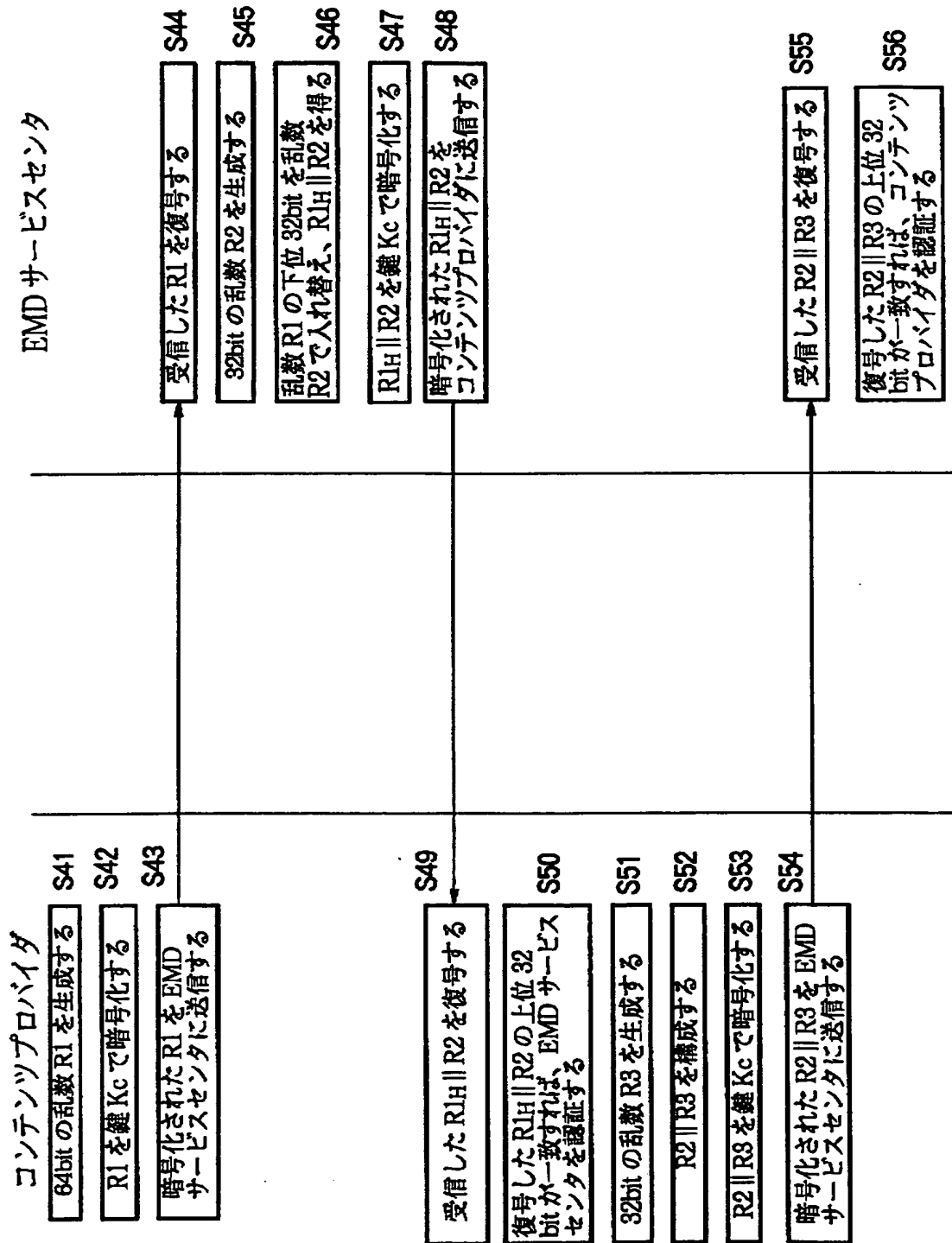
【図 40】



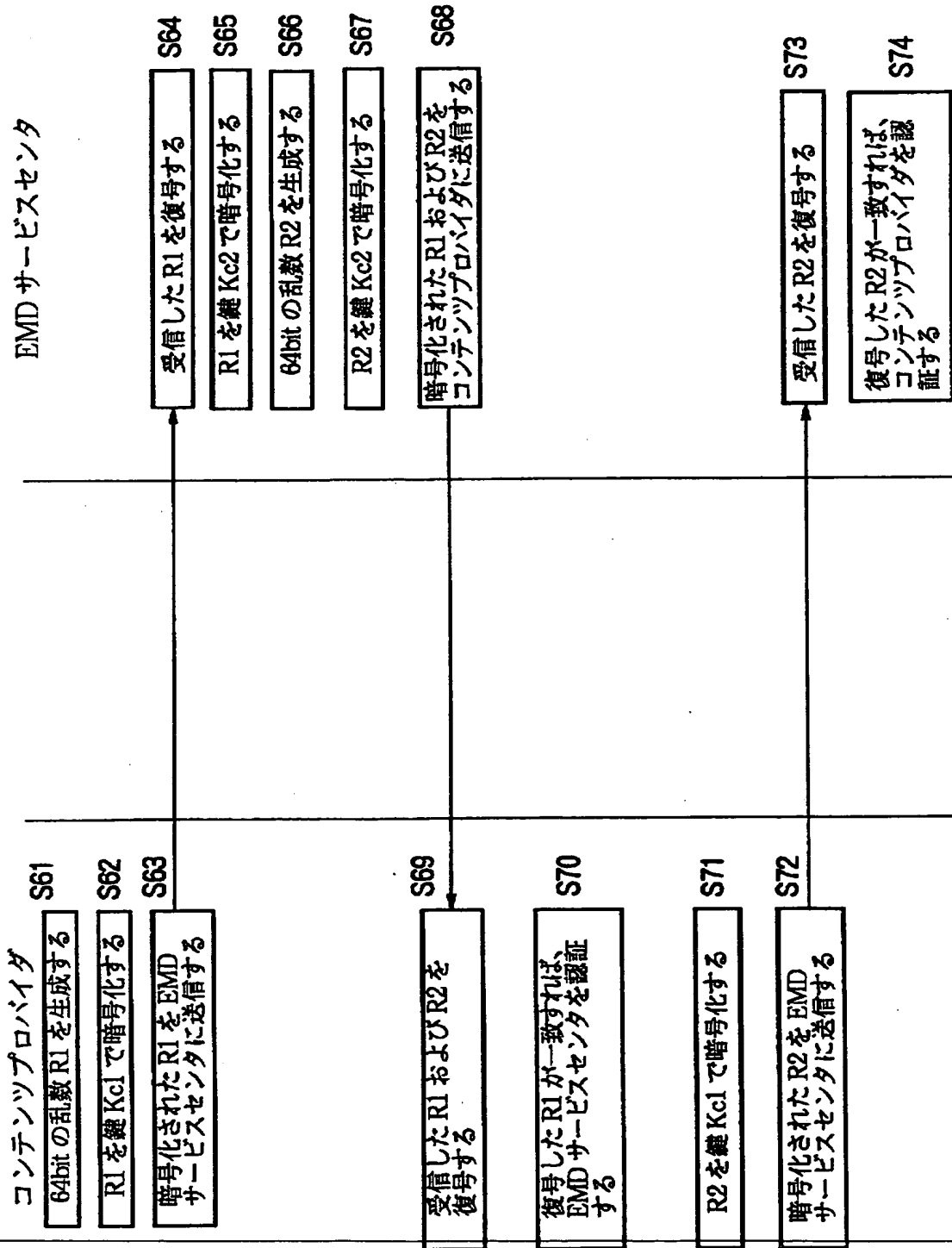
【図 4 1】



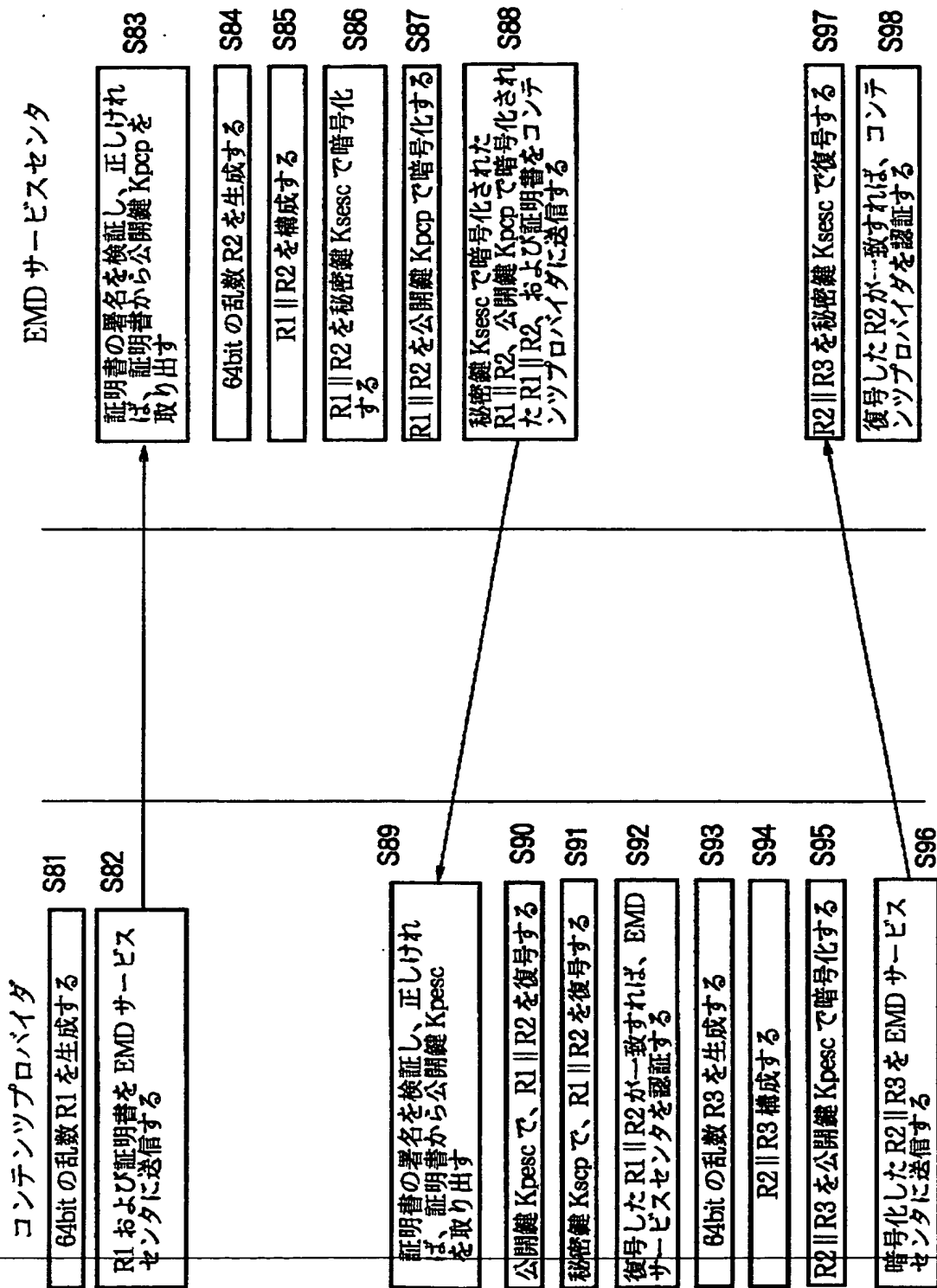
【図 4 2】



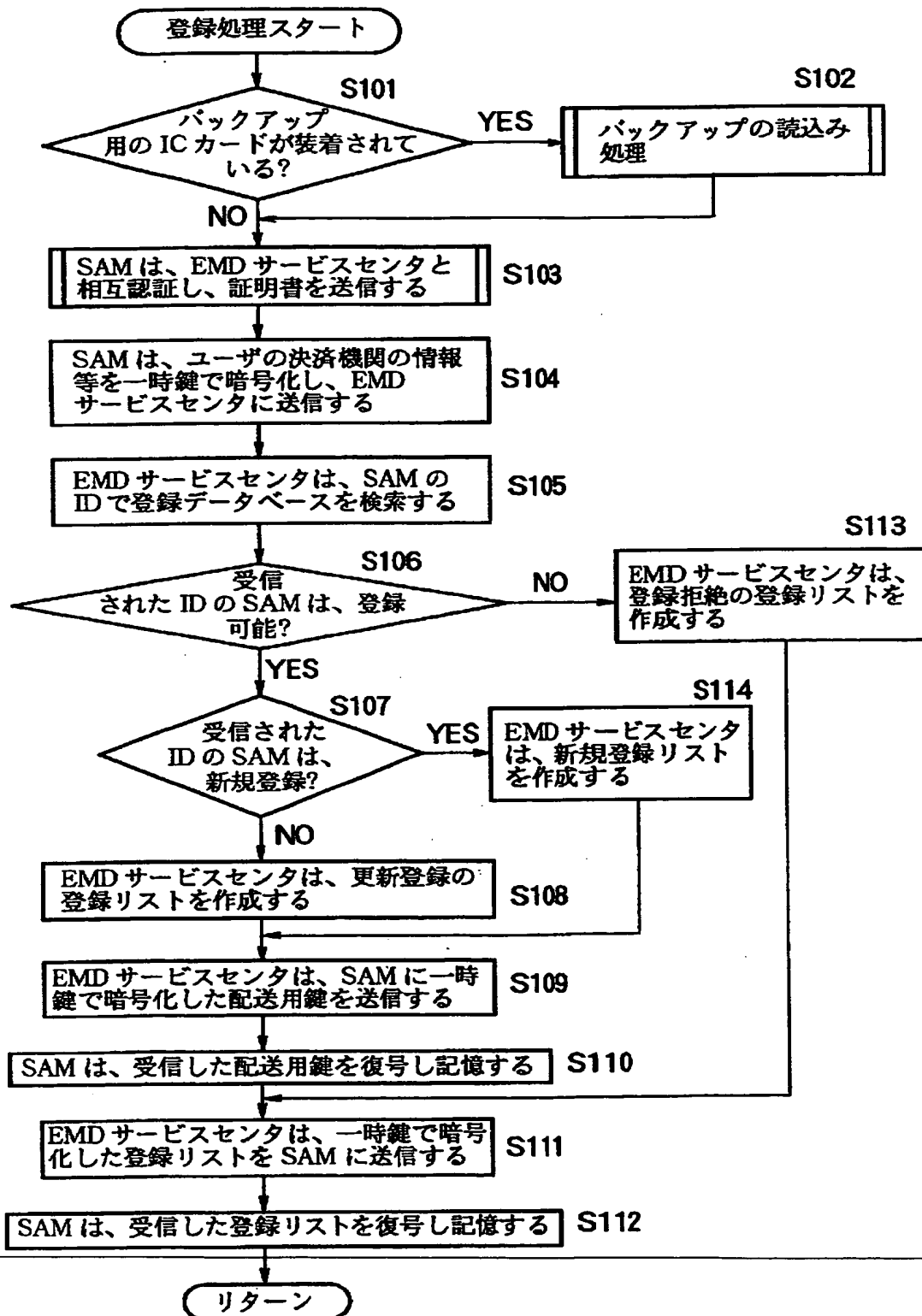
【図 43】



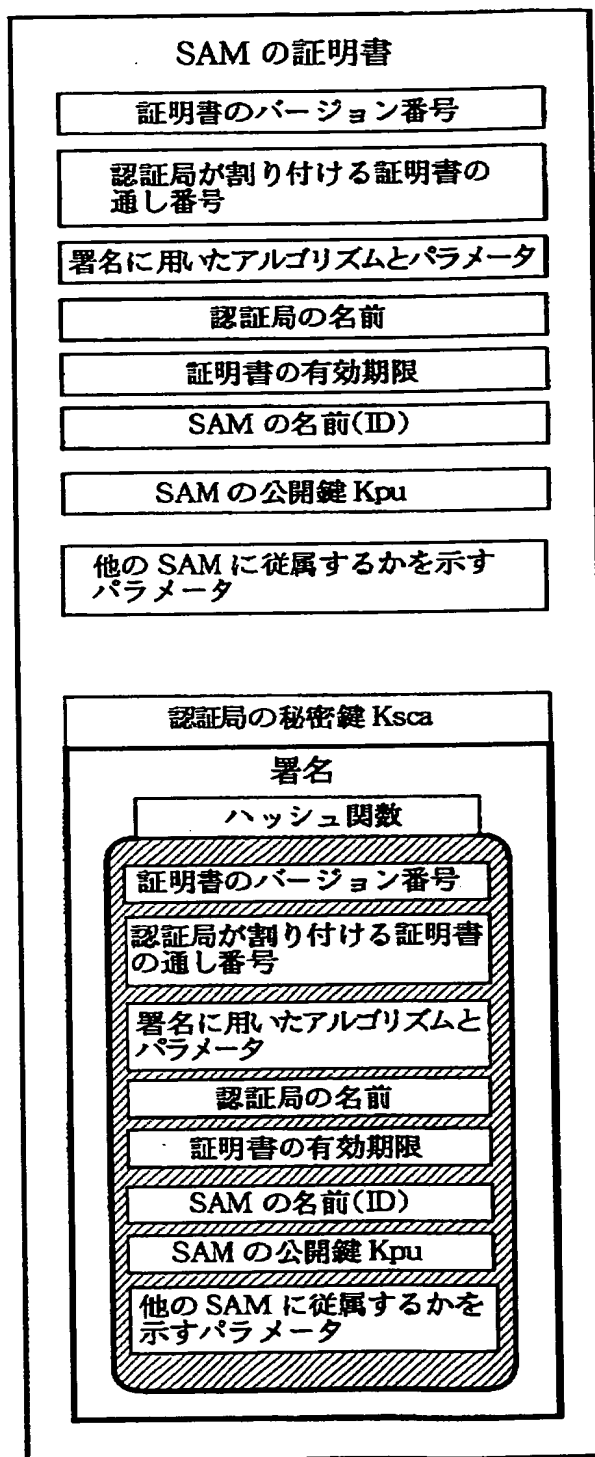
【図 4 4】



【図 45】



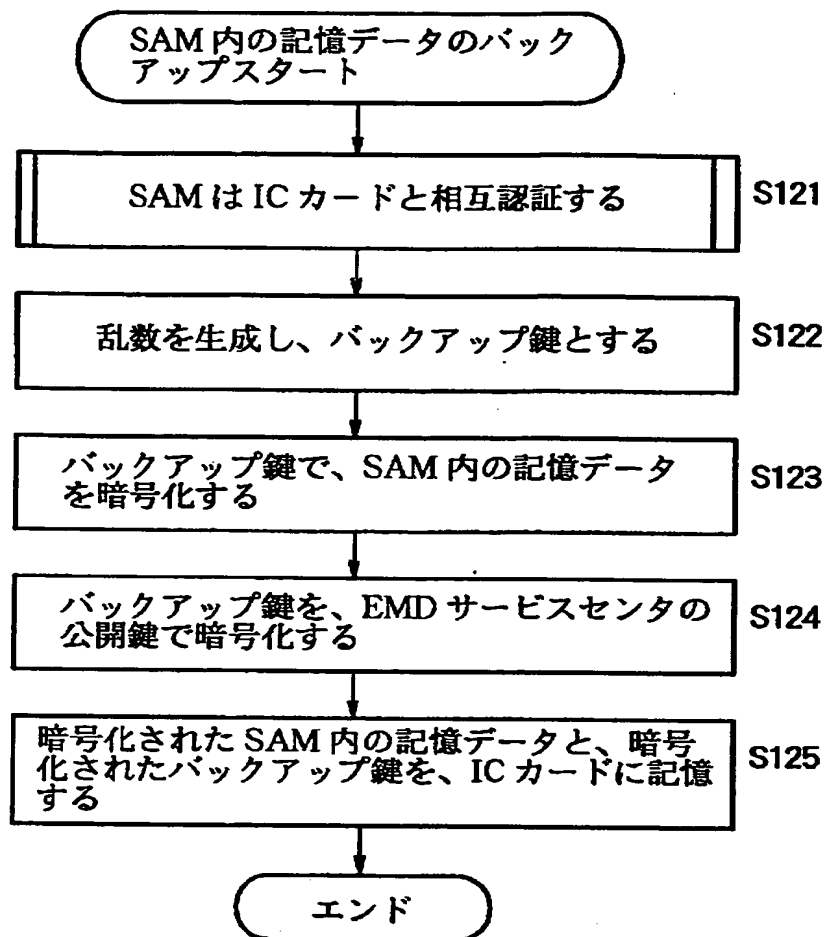
【図 46】



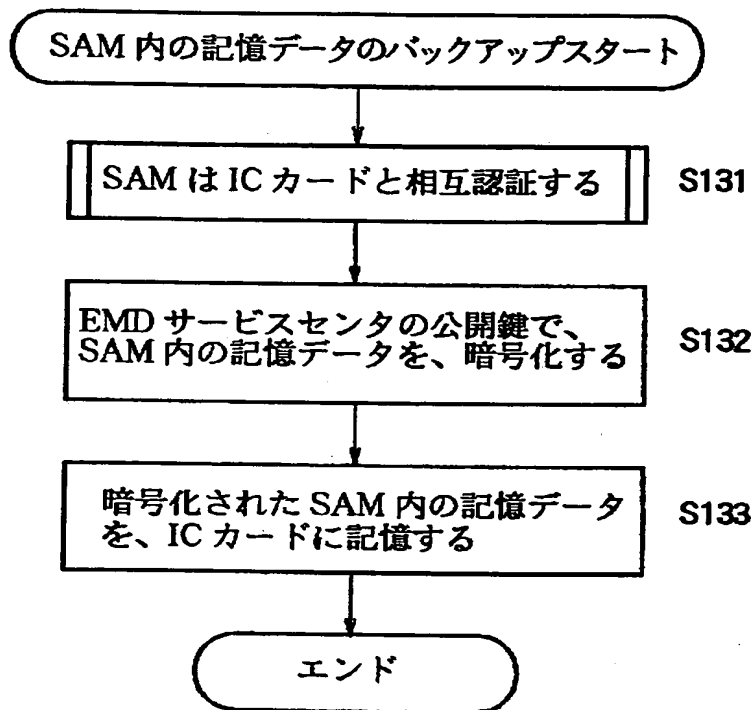
【図 4 7】

[illegible]

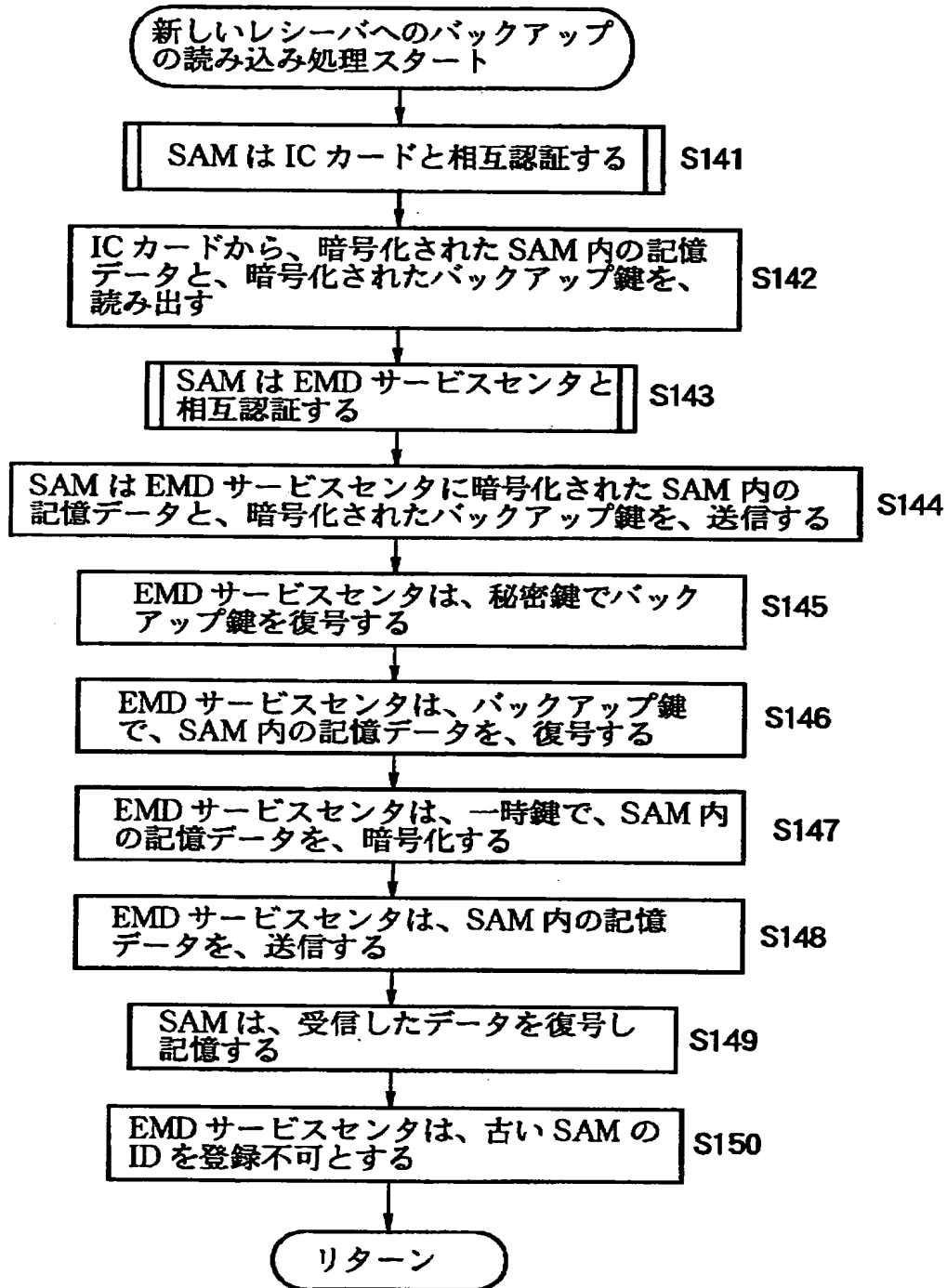
【図 48】



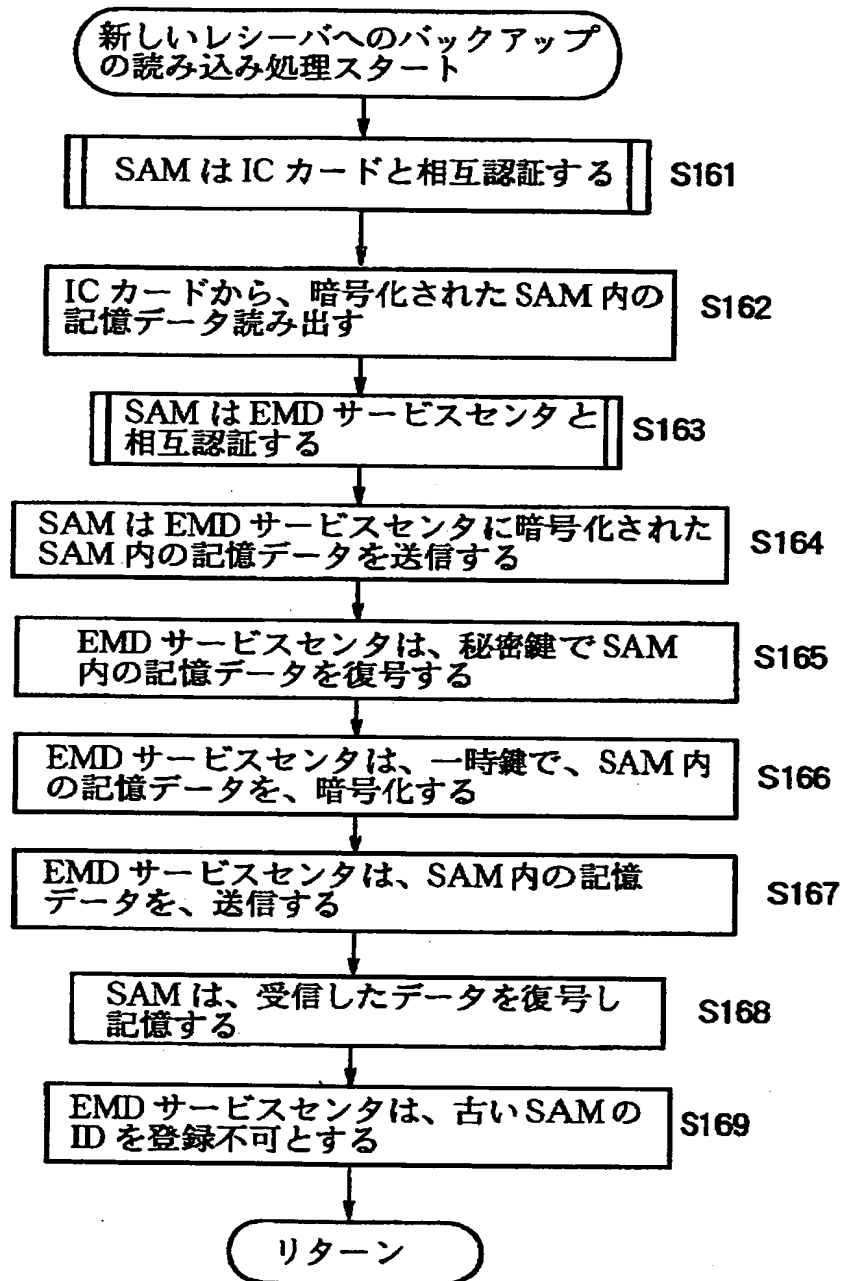
【図 49】



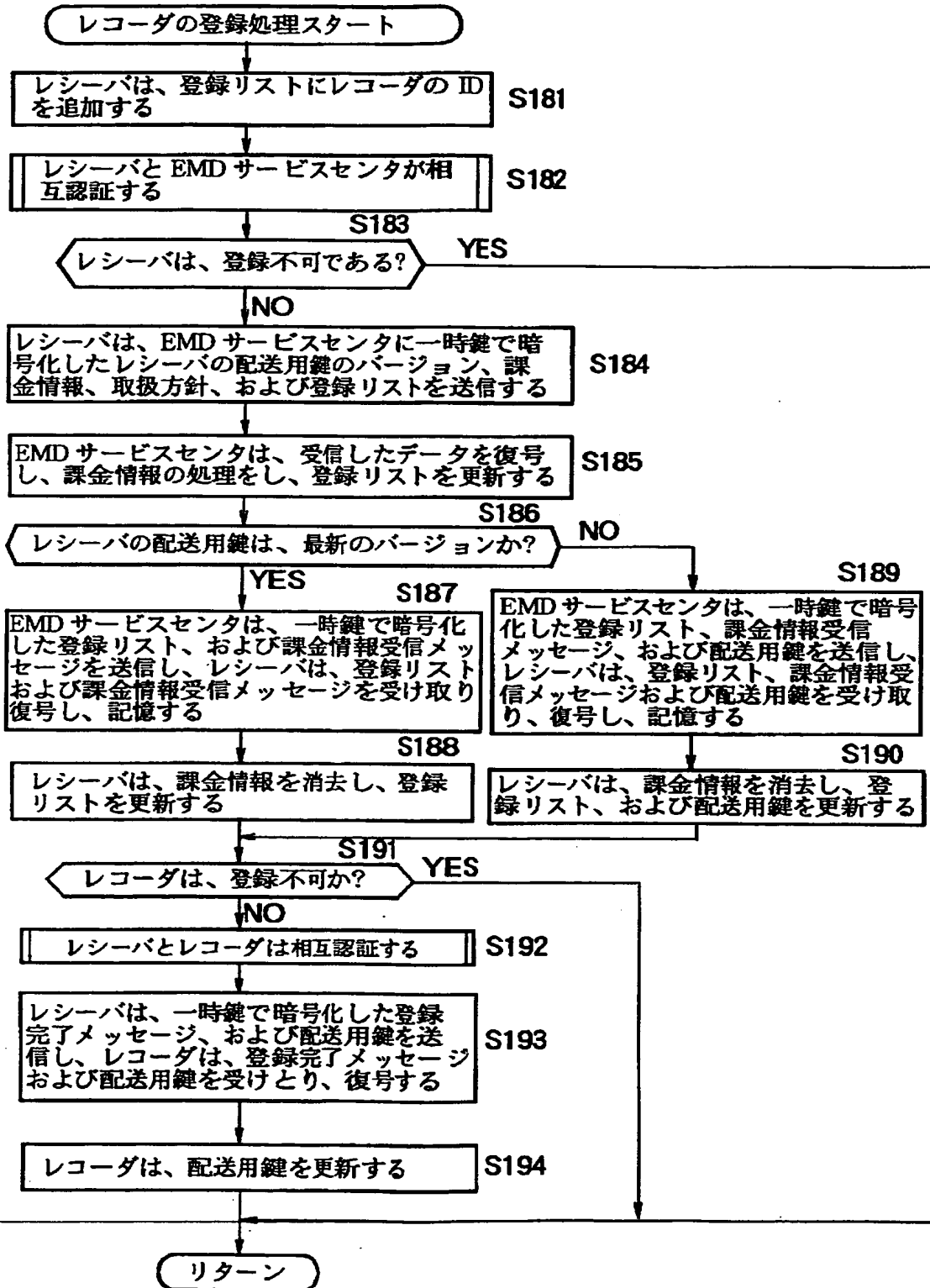
【図 50】



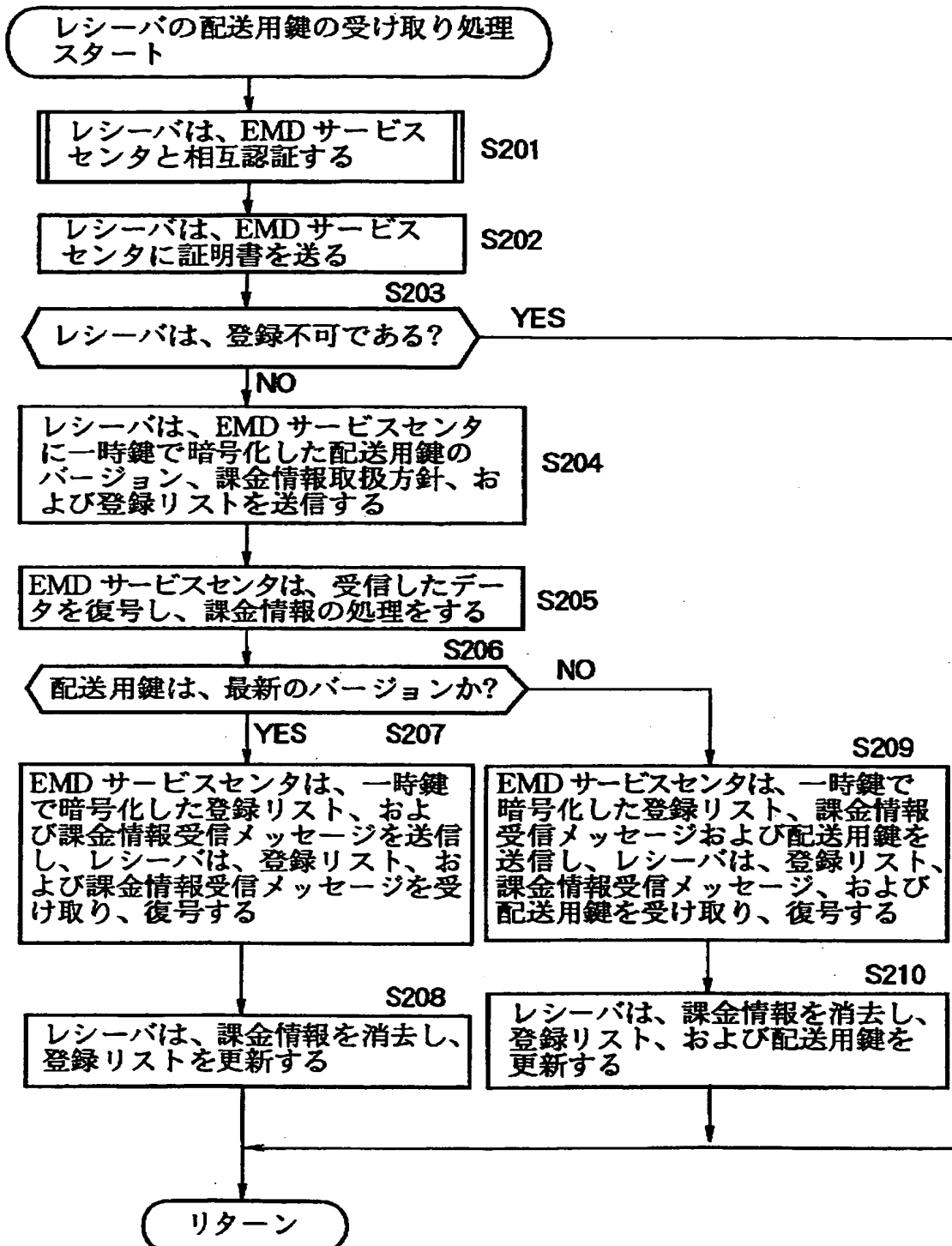
【図 5 1】



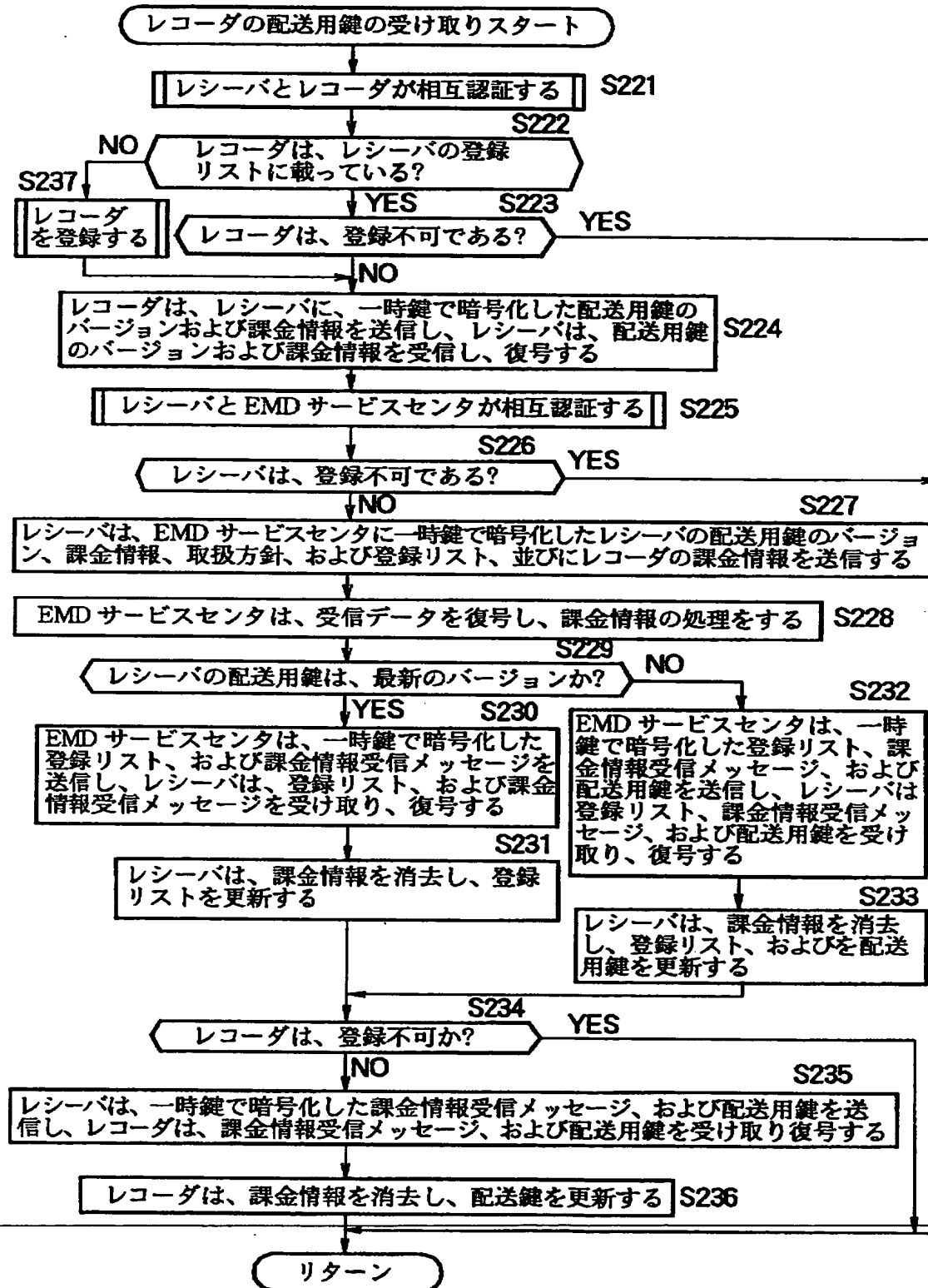
【図 5 2】



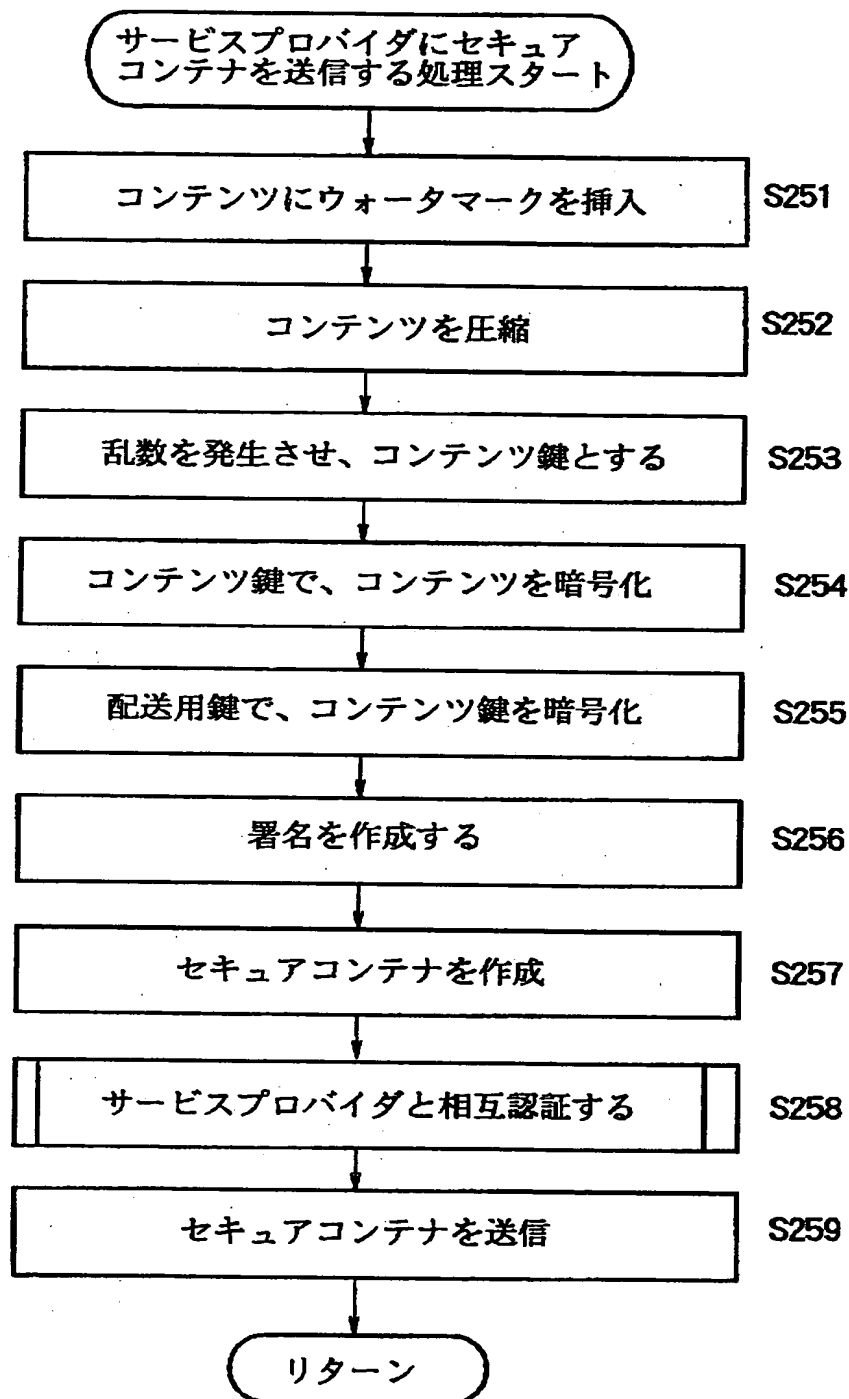
【図53】



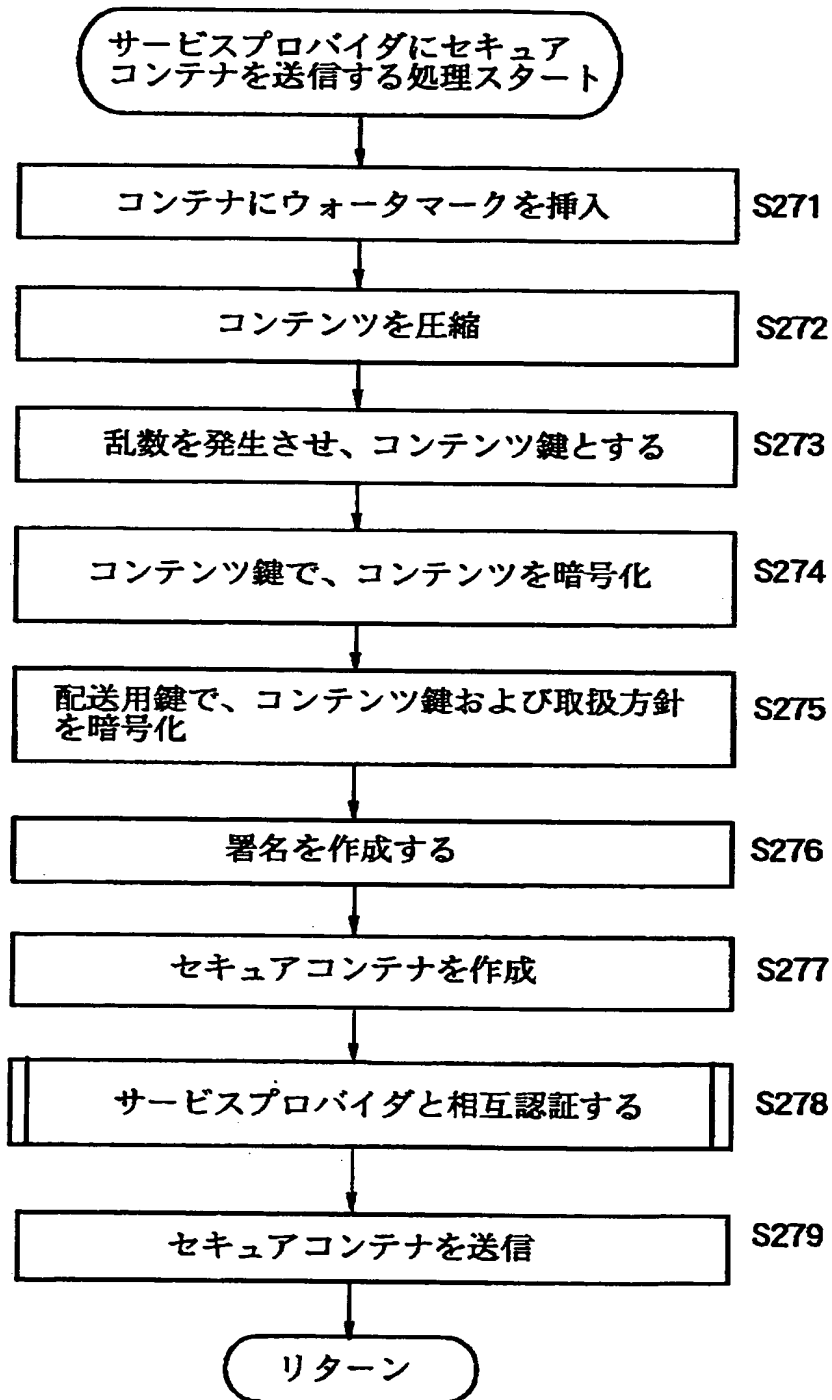
【図 5 4】



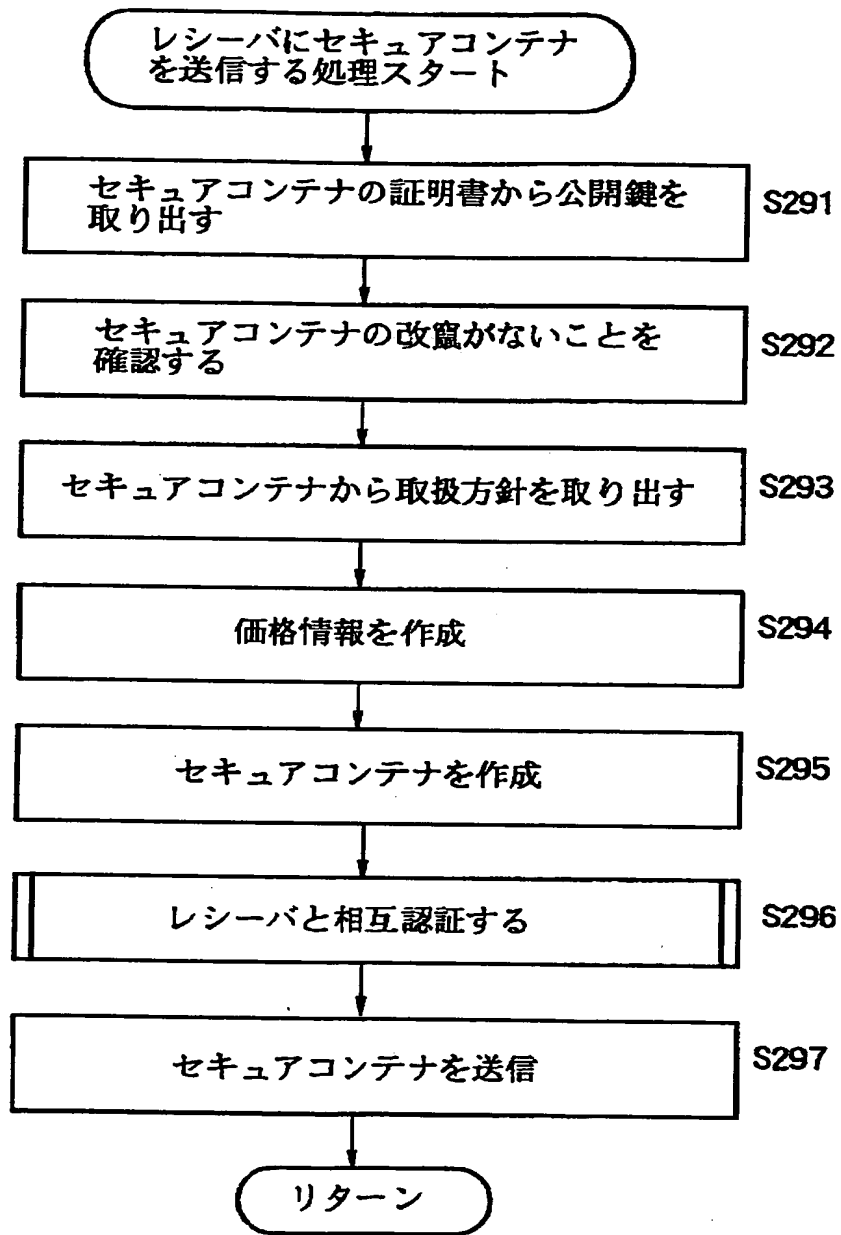
【図 55】



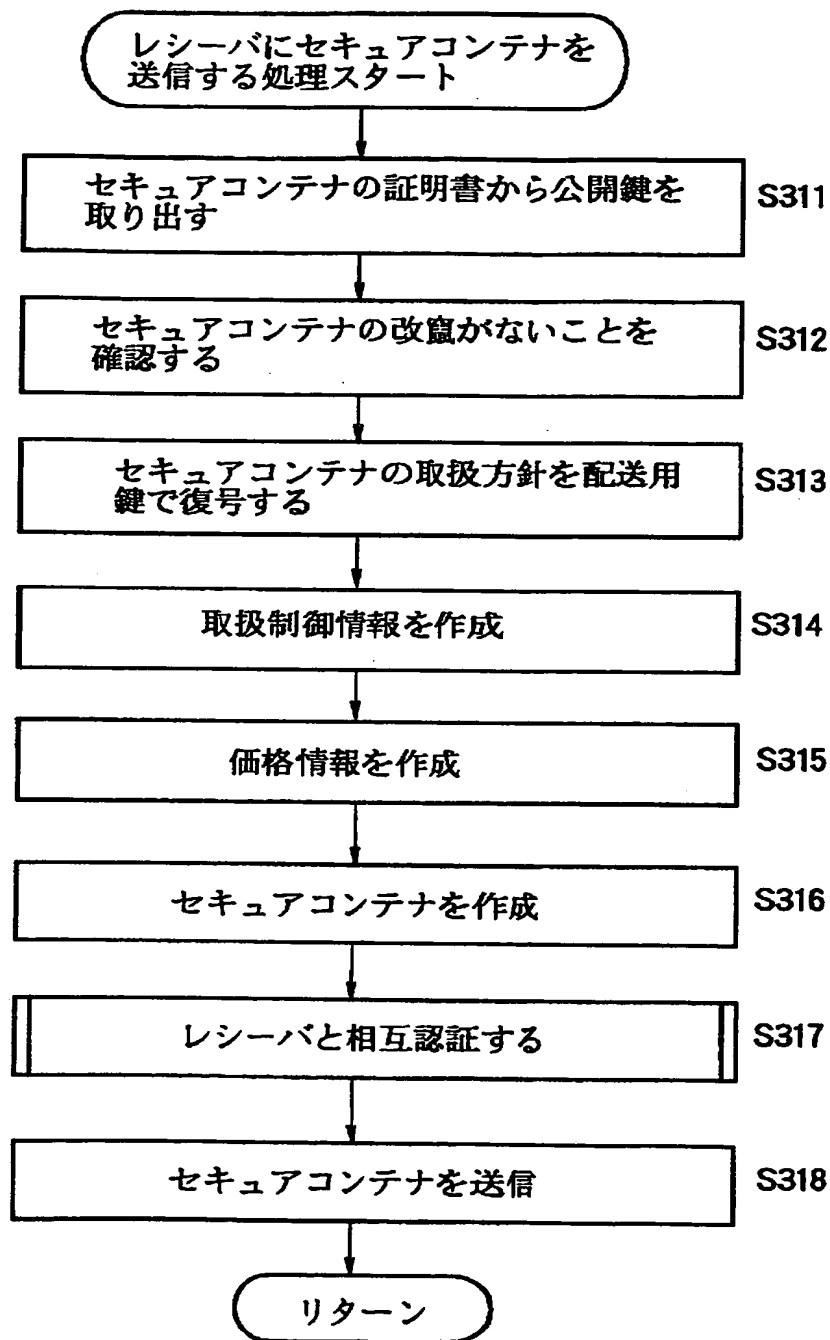
【図 56】



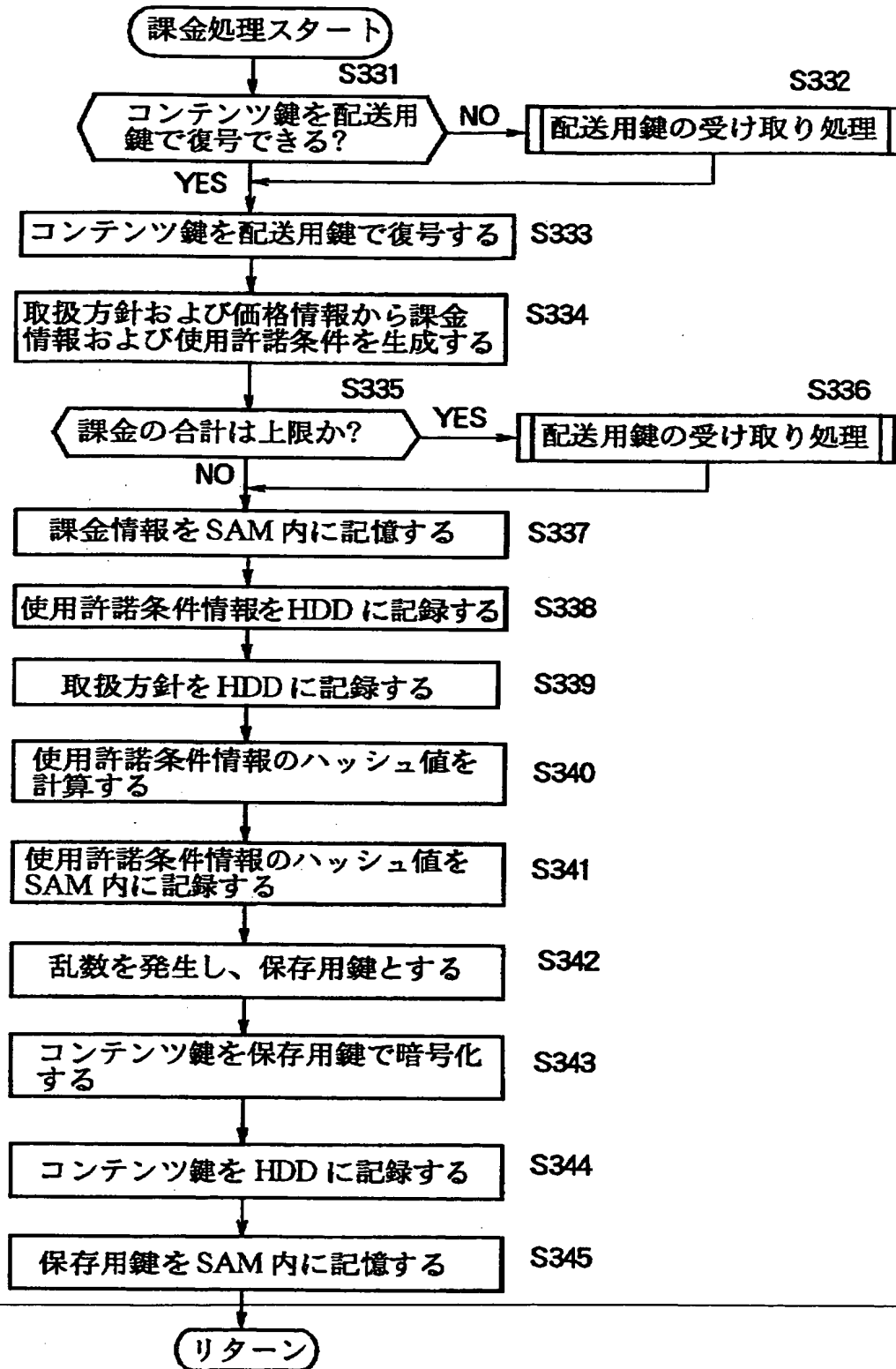
【図 57】



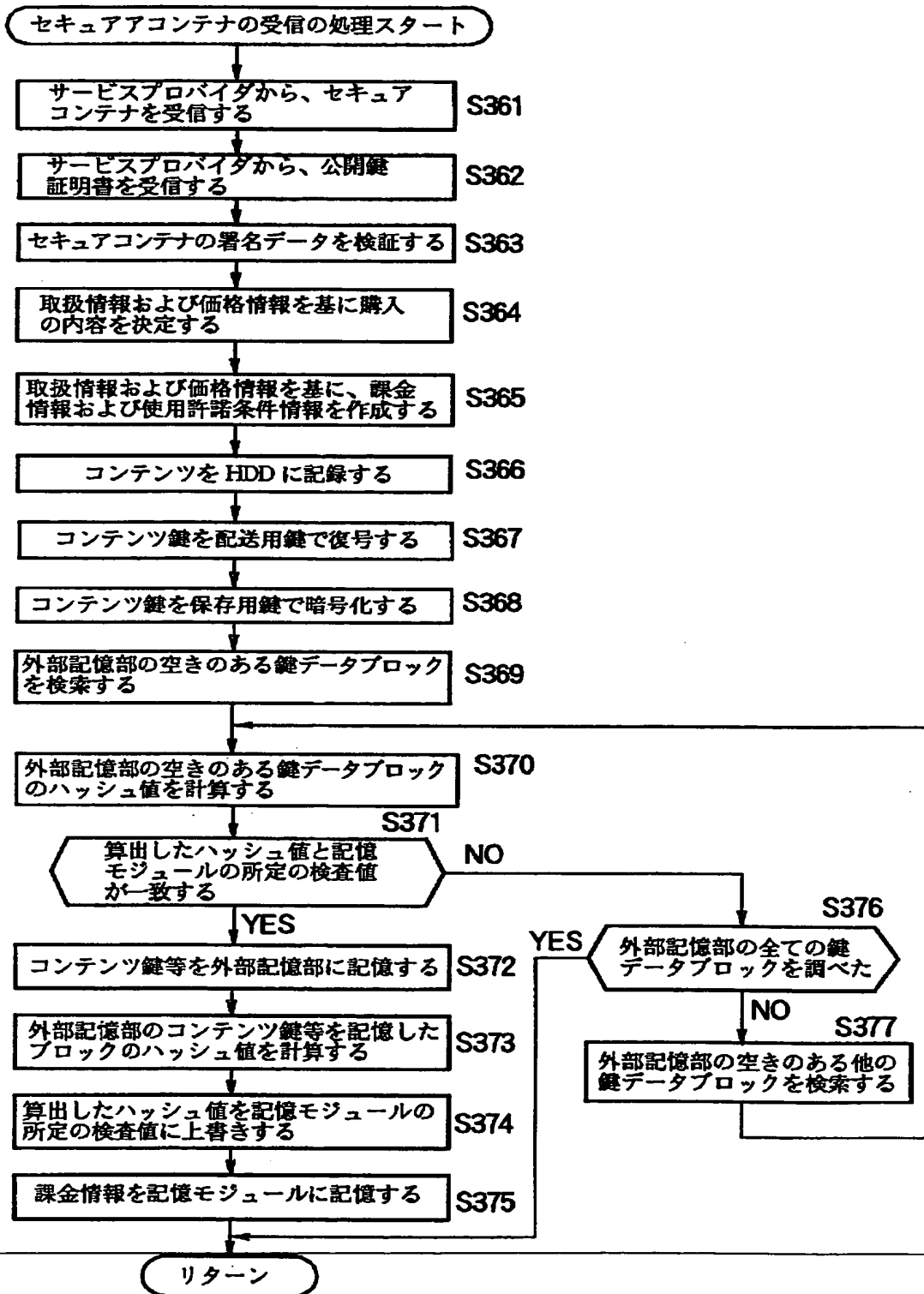
【図 58】



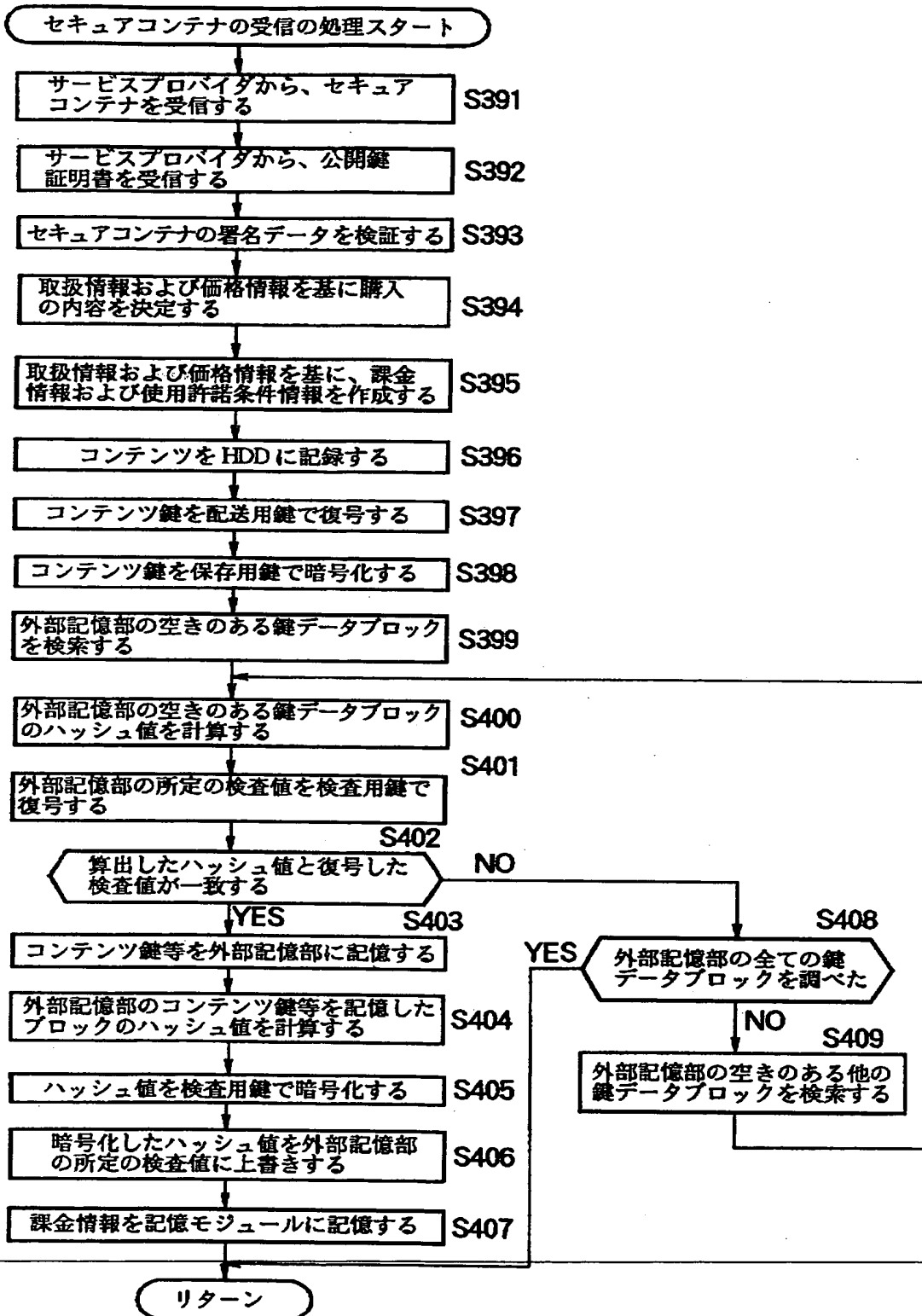
【図 59】



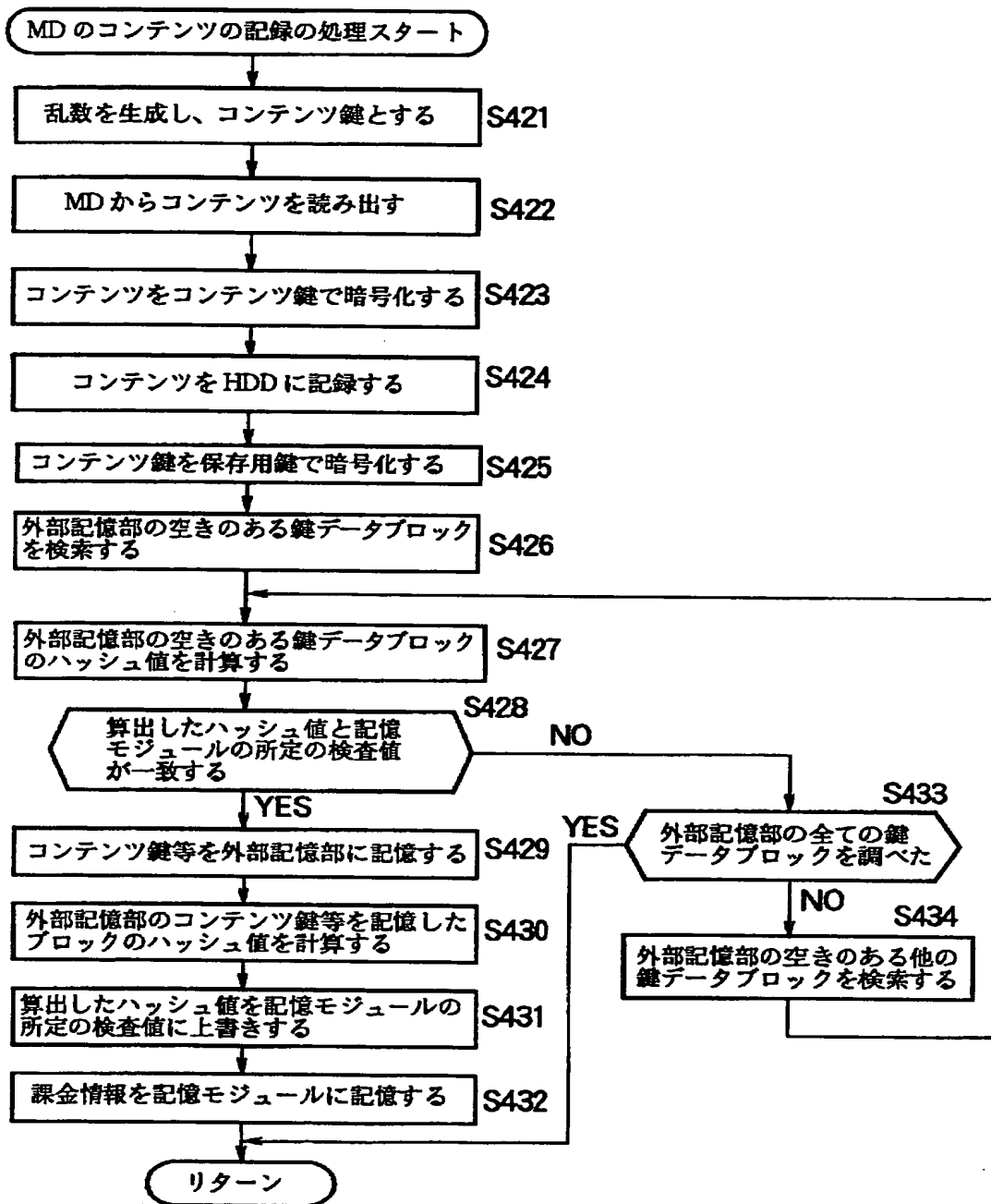
【図 60】



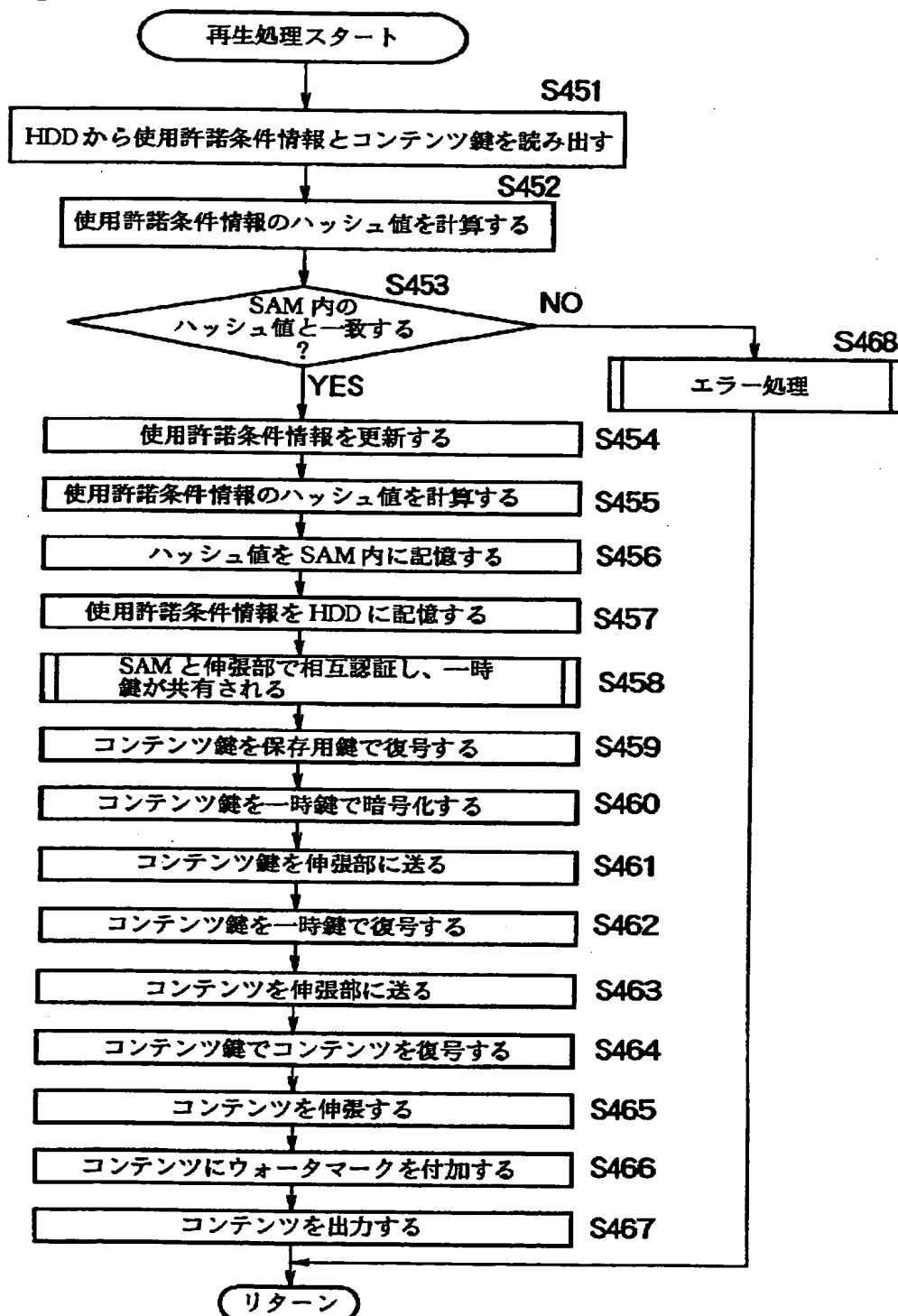
【図 61】



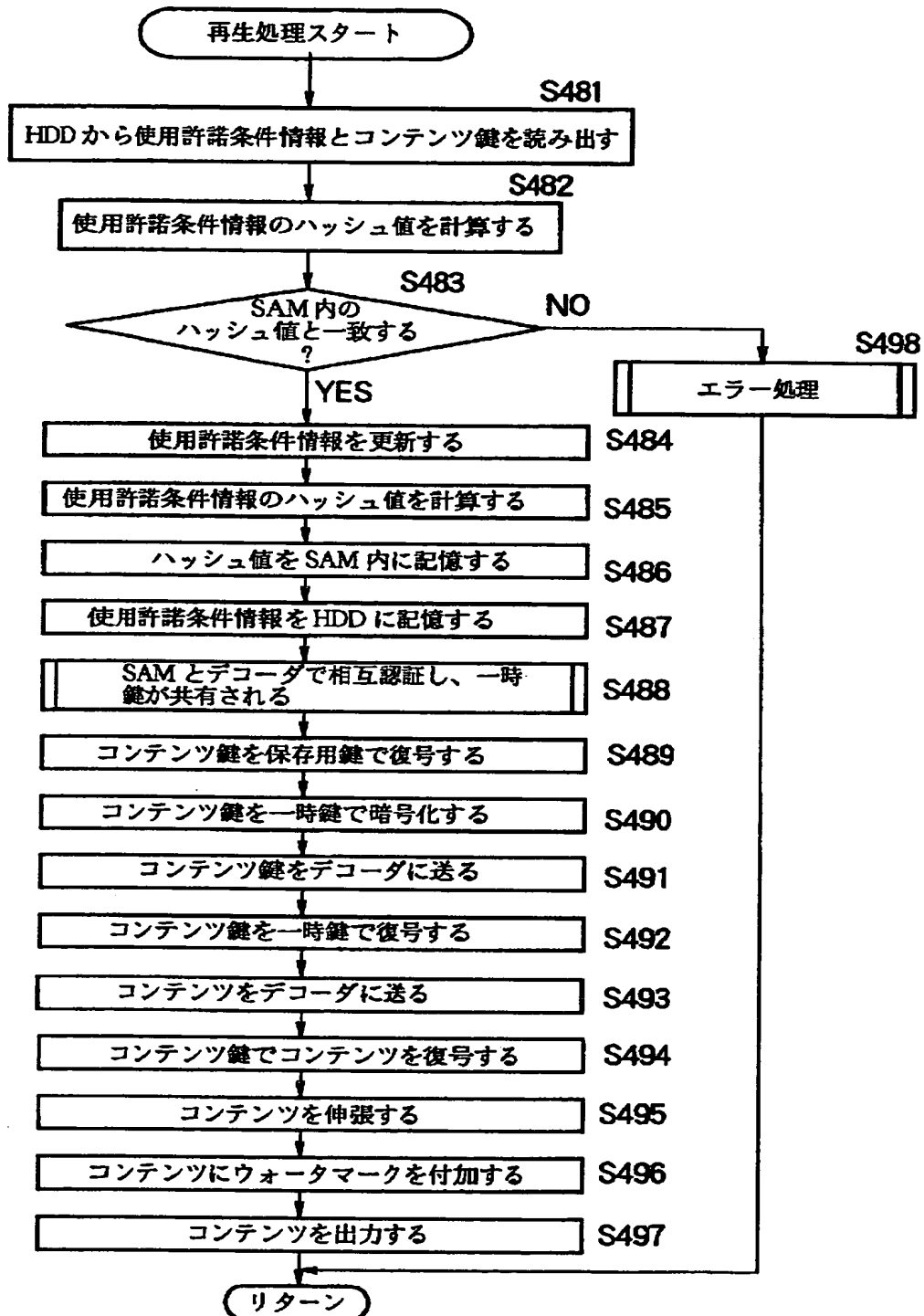
【図 6 2】



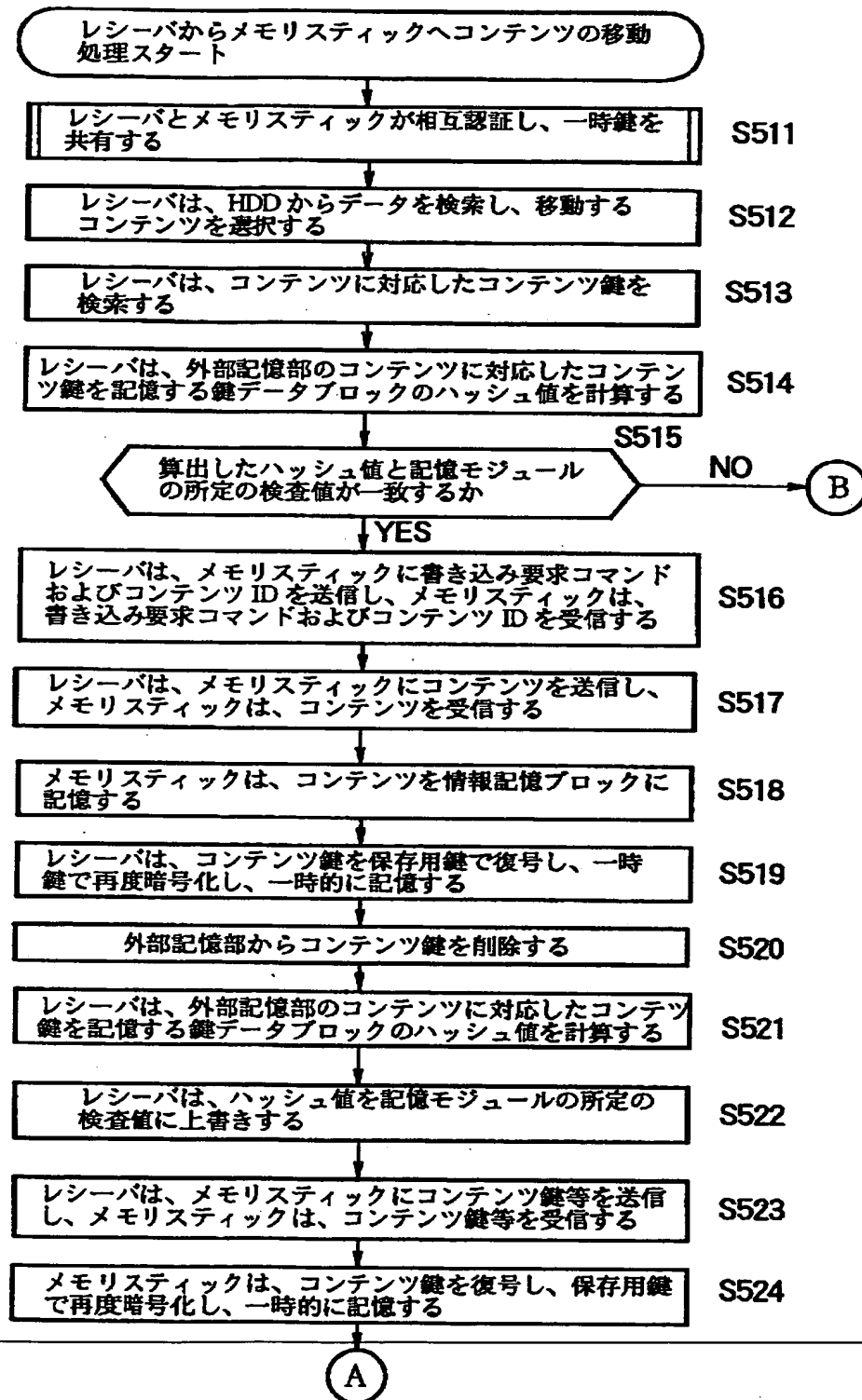
【図 63】



【図 6 4】

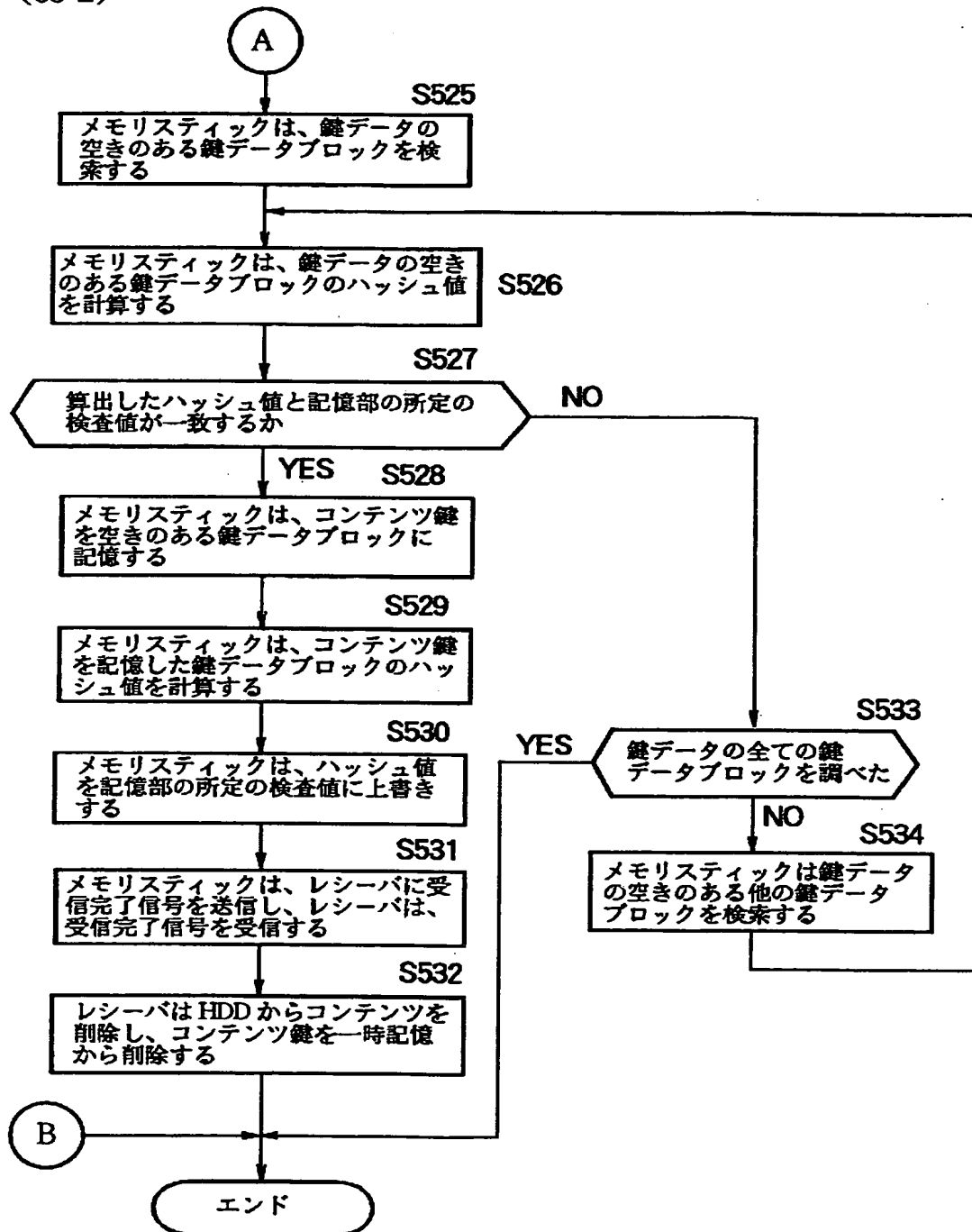


【図 65】
(65-1)



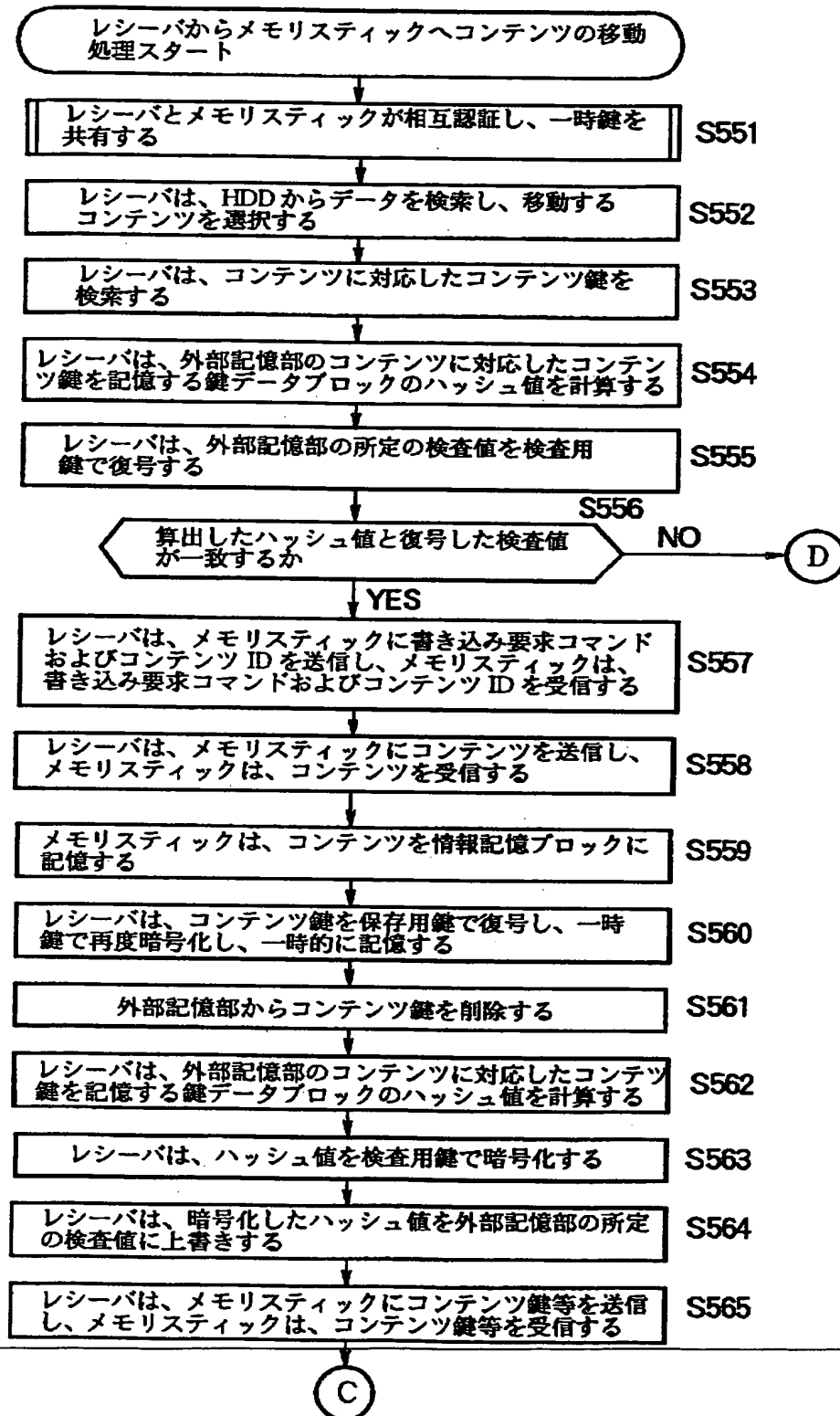
【図 66】

(65-2)

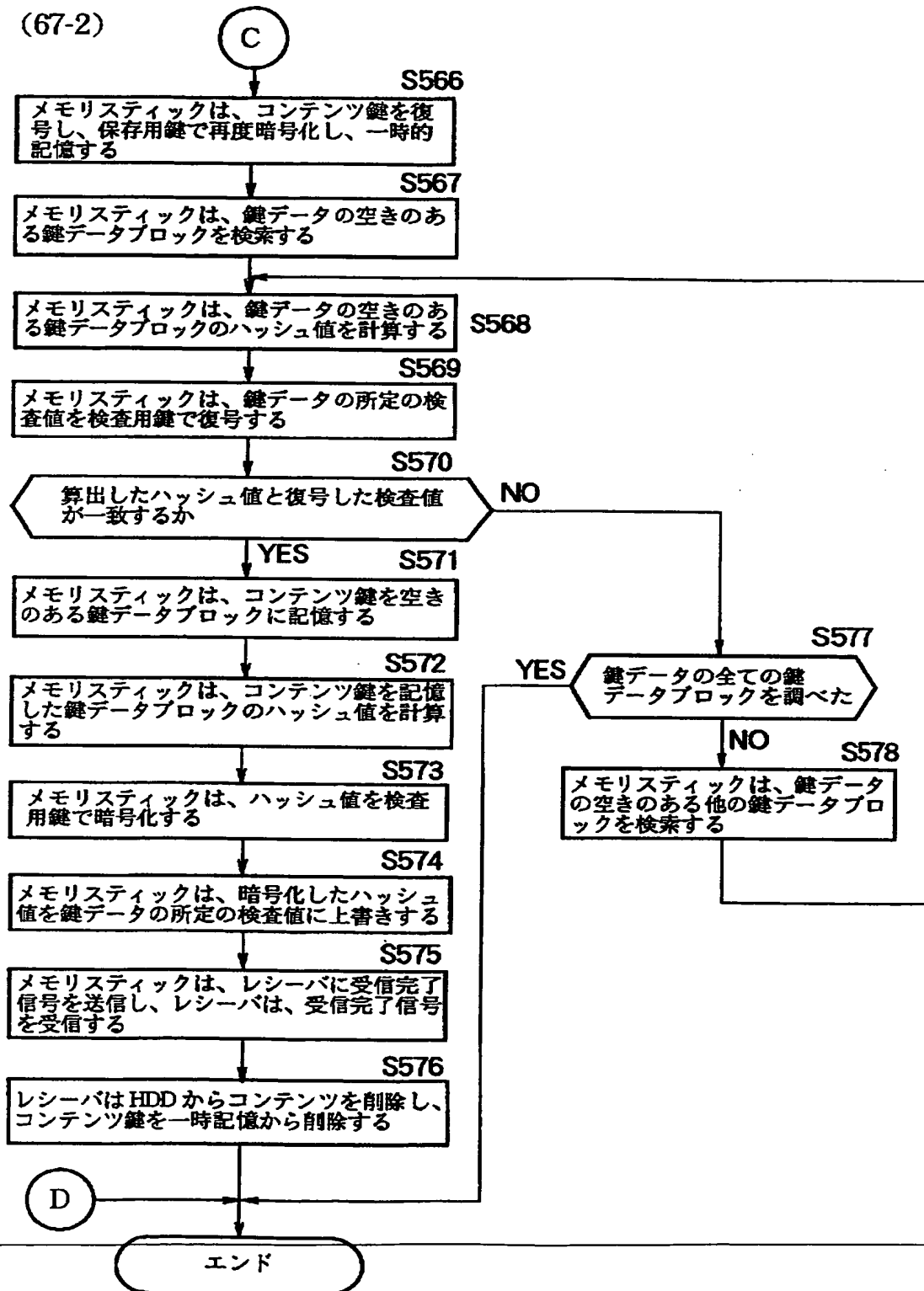


【図 6 7】

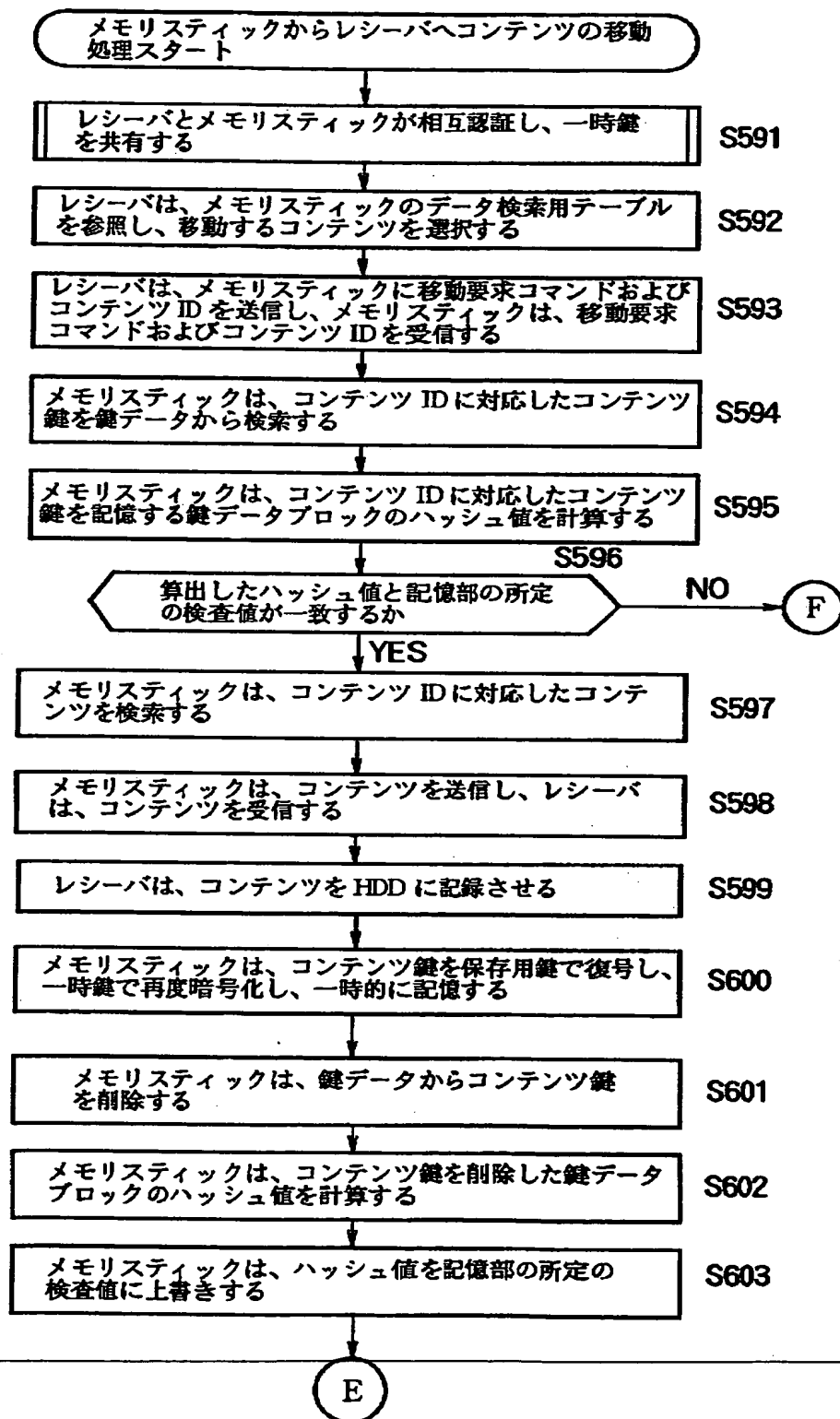
(67-1)



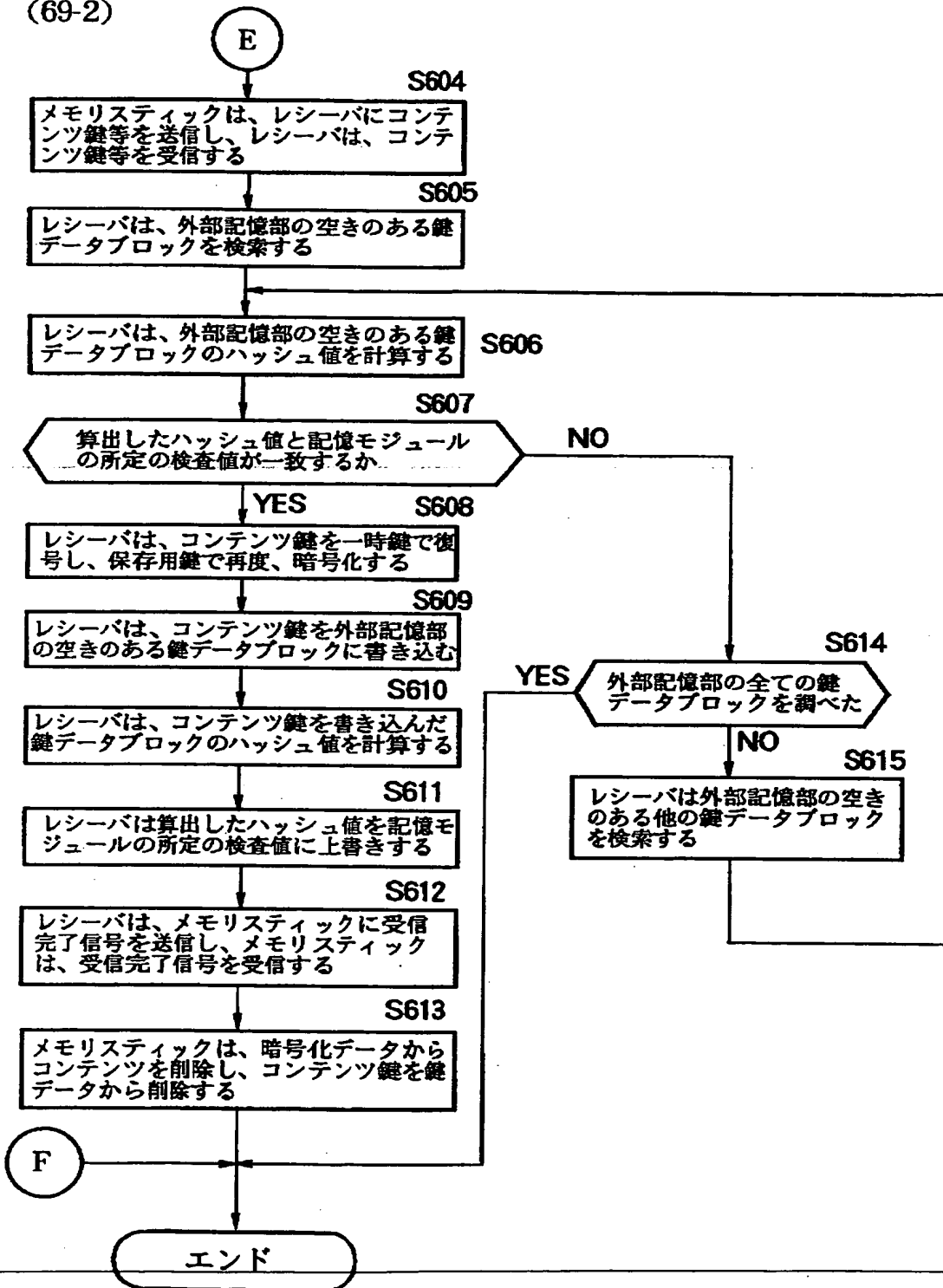
【図 68】
(67-2)



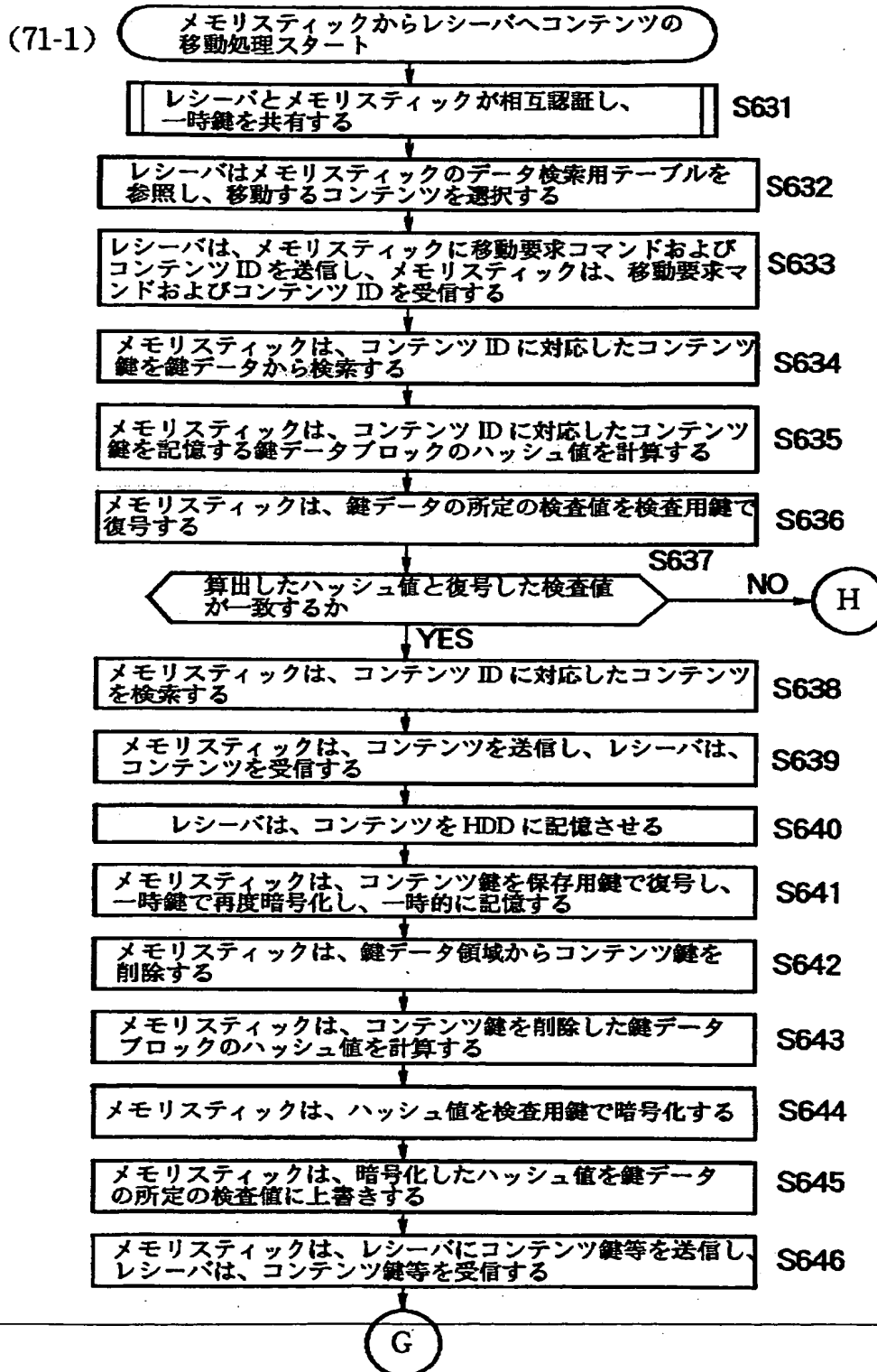
【図 69】
(69-1)



【図70】
(69-2)

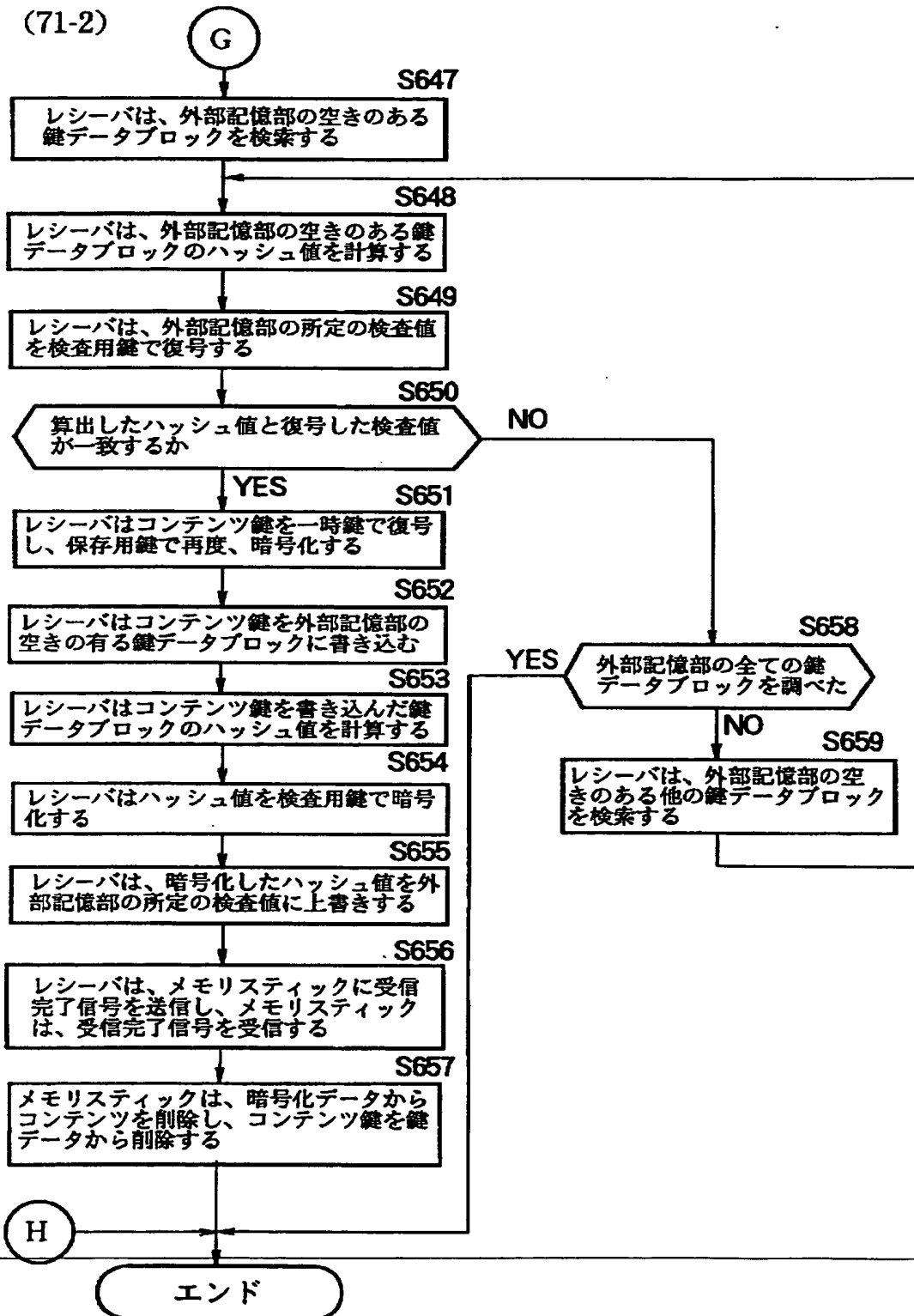


【図 7 1】

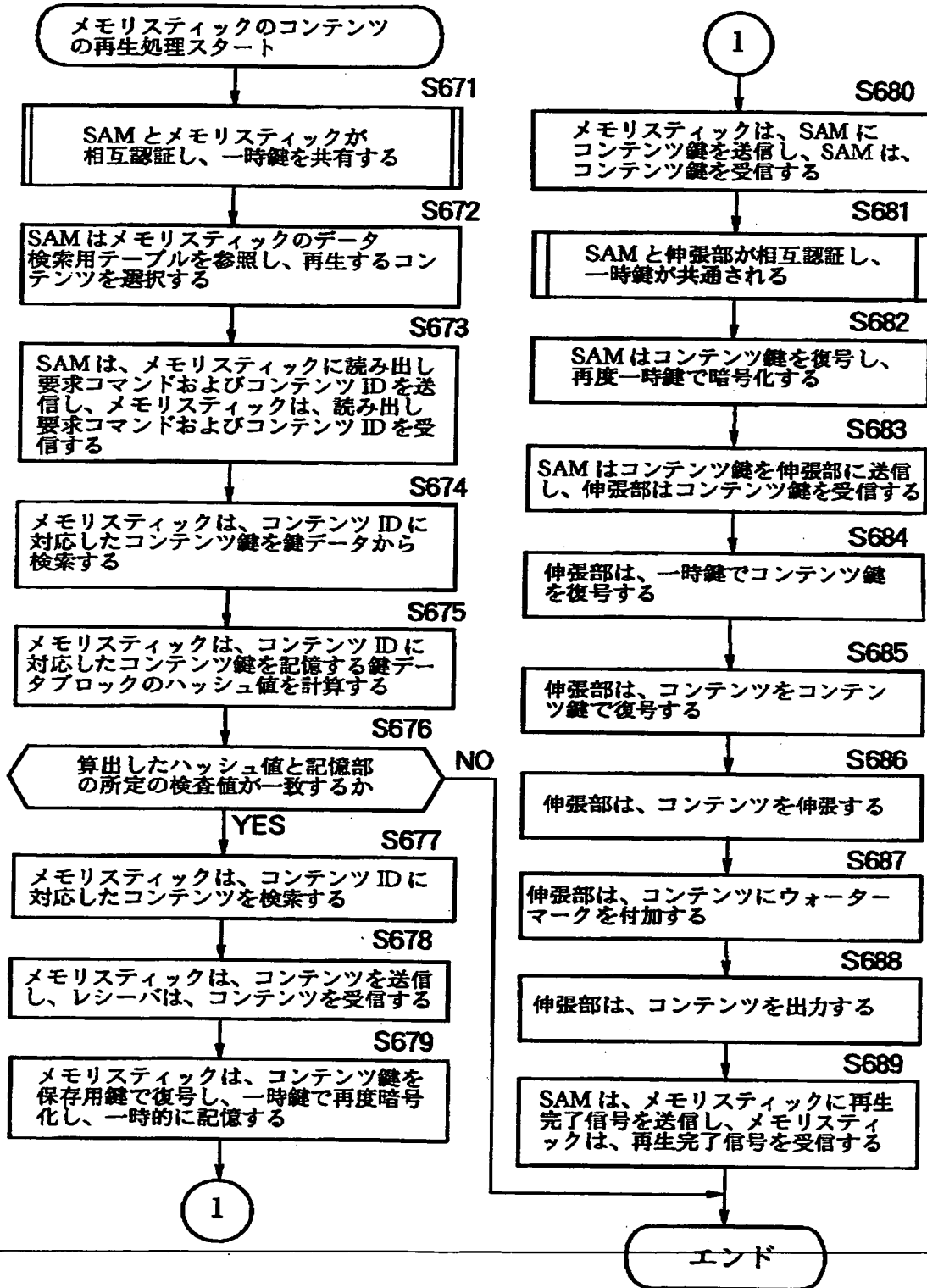


【図 7 2】

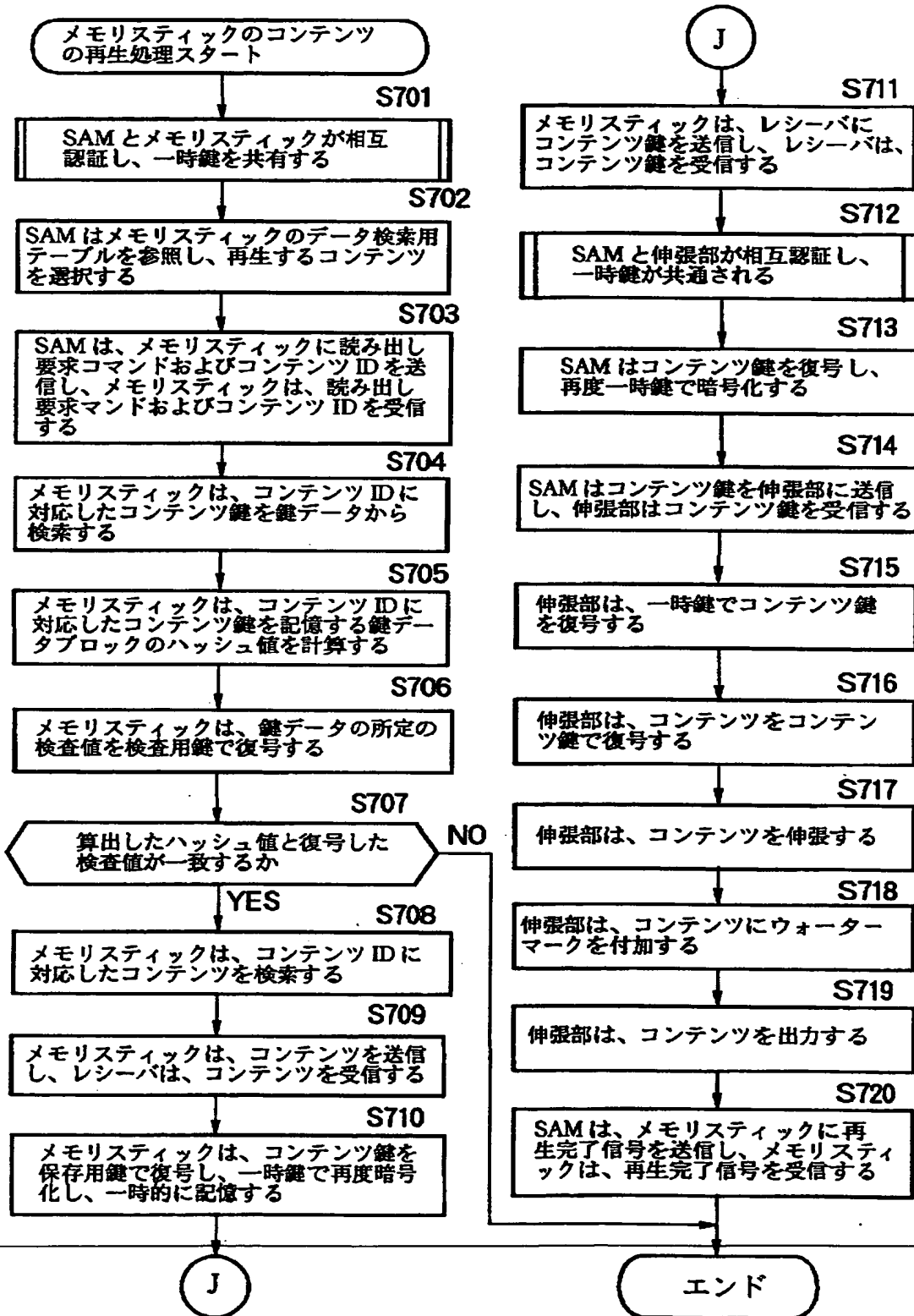
(71-2)



【図 7 3】



【図 74】



【書類名】 要約書

【要約】

【課題】 情報の利用内容を示す情報の書き換えを検知する。

【解決手段】 課金処理モジュール72は、情報の使用の許諾条件を示す情報を生成し、復号／暗号化モジュール74は、許諾条件を示す情報の認証情報を生成し、記憶モジュール73は、認証情報を記憶する。

【選択図】 図10

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】
【識別番号】 000002185
【住所又は居所】 東京都品川区北品川6丁目7番35号
【氏名又は名称】 ソニー株式会社
【代理人】 申請人
【識別番号】 100082131
【住所又は居所】 東京都新宿区西新宿7丁目5番8号 GOWA西新
宿ビル6F 稲本国際特許事務所
【氏名又は名称】 稲本 義雄

出 願 人 履 歴 情 報

識別番号

[000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社